Hcon Security Testing Framework Manual

Version 0.5 revision 1

Ashish Mistry

About the Author

Ashish Mistry

He is the author of Hcon Security Testing Framework (HconSTF). His area of expertise are web application penetration testing, open source intelligence and malware analysis with more than 6 years of experience in IT security industry for providing training and security solutions for corporates and educational institutes.

Dedicated to my loving parents and my supportive brother

without whom this book would not have possible

Acknowledgments

A huge thanks to all of the Add-ons, scripts developers for making HconSTF possible. I would like to thank Aj Rebel for helping and giving ideas for HconSTF v0.1 Aqua base. Also thanks to the awesome HconSTF community people who supported and shared it and made it this big.

Preface

This book is written for using with HconSTF v0.5 codename 'Prime', but can be used with HconSTF v0.4 codename 'Freedom' with few limitations. The purpose of this book is to be an All-in-One resource for HconSTF users offering how to utilize it and perform different security assessment related tasks efficiently and quickly. There is no exhaustive explanation of things or techniques but rather it is straight to the point for doing a particular task. The covered content in this book is a blend of User Manual, How-To and Tutorial format.

This book is published as a rolling release this means that with every new version of HconSTF there will be a new version of book, and the book will be periodically updated and improved with revisions.

Copyright and Legal Information

Copyright © 2014 Ashish Mistry | Hcon.in

All rights reserved. No part of this work should be reproduced or transmitted in any form or by any means, without prior written permission of the copyright owner.

The information in this book is distributed “as is”. While every precaution was taken to ensure the accuracy of the material, the author assumes no responsibility or liability for error or omissions, or for damages resulting from the use of the information contained herein.

Table of Contents

Chapter 1: Introduction ….....9
1.1 What is HconSTF ….....10
1.2 Core Architecture & Design Guidelines ….....10
1.3 Different Editions ….....11
Chapter 2: Origin of HconSTF ….....13
2.1 Inspiration 14
2.2 Initial Release ….....14
2.3 First Public Release ….....15
Chapter 3: Getting Started with HconSTF ….....16
3.1 Prerequisites ….....17
3.2 Downloading HconSTF ….....17
3.3 Setting all up ….....18
3.4 Familiarization with User Interface ….....21
3.5 Customizing Preferences ….....27
3.5.1 Configuring Reporting ….....37
3.6 Updating HconSTF ….....40
Chapter 4: The Arsenal ….....42
4.1 Categories of Tools ….....43
4.2 Special Features ….....45
4.3 Miscellaneous: Extras Directory & HconSTF Cleaner ….....50
4.4 Tools Listing ….....51
4.4.1 Add-ons ….....51
4.4.2 Search Aggregator Plugins ….....52
4.4.3 GreaseMonkey Scripts ….....54
Chapter 5: Web Application Penetration Testing with HconSTF ….....55
5.1 Information Gathering & Initial Analysis ….....56
5.1.1 Mapping ….....56
5.1.2 Reconnaissance ….....59
5.1.3 Metadata Analysis ….....69

5.2 Testing for Vulnerabilities ….....72
5.2.1 Cross Site Scripting (XSS) ….....72
5.2.2 SQL Injection (SQLi) ….....78
5.2.3 File Upload Vulnerability ….....82
5.3 Request Manipulation ….....88
5.3.1 Inspecting Request ….....88
5.3.2 Intercepting Request ….....92
5.3.3 Replaying Request ….....93
5.3.4 Crafting Custom Request ….....96
Chapter 6: Cryptography ….....101
6.1 Hashing/Encoding/Decoding ….....102
6.2 Identifying Unknown Hash ….....105
6.3 Cracking Hashes 106
Chapter 7: Anonymity ….....110
7.1 User Agent Spoofing ….....111
7.2 Header Spoofing ….....115
7.3 Darknets & Proxies ….....119
Chapter 8: Connecting with Other Tools ….....127
8.1 Custom Tool on Ipprotocols ….....128
Chapter 9: Troubleshooting ….....134
9.1 Tools Not Working From WebUI & Search Aggregator ….....135
9.2 Missing Status Bar and H-menu ….....135
9.3 “Another Instance of HconSTF is Already Running” error ….....137
Chapter 10: Getting Further information & Help ….....138
10.1 More Resources on HconSTF ….....139
10.2 Contribute in HconSTF ….....139
10.3 Learn Web Application Pentesting with HconSTF ….....140

Chapter 1: Introduction

In this chapter we will going to understand basically what HconSTF is and what are its core design ideas and workings with difference in its main editions.

1.1 What is HconSTF

HconSTF stands for Hcon Security Testing Framework which is a semi-automated open source security assessment toolset which can perform various tasks related to,

- Web Penetration Testing
- Web Exploits Development
- Web Malware Analysis
- Open Source Intelligence (Cyber Spying & Doxing)

The whole framework uses different web technology clients as its development base platforms and further customizes it for security assessment needs.

HconSTF is *not* a point-click-forget tool. For using it to its maximum capabilities users need to have the most powerful engine called your own brain.

1.2 Core Architecture & Design Guidelines

As seen in the figure below HconSTF follows layered design architecture on different web client technologies, this gives more flexibility in development and less compatibility issues.

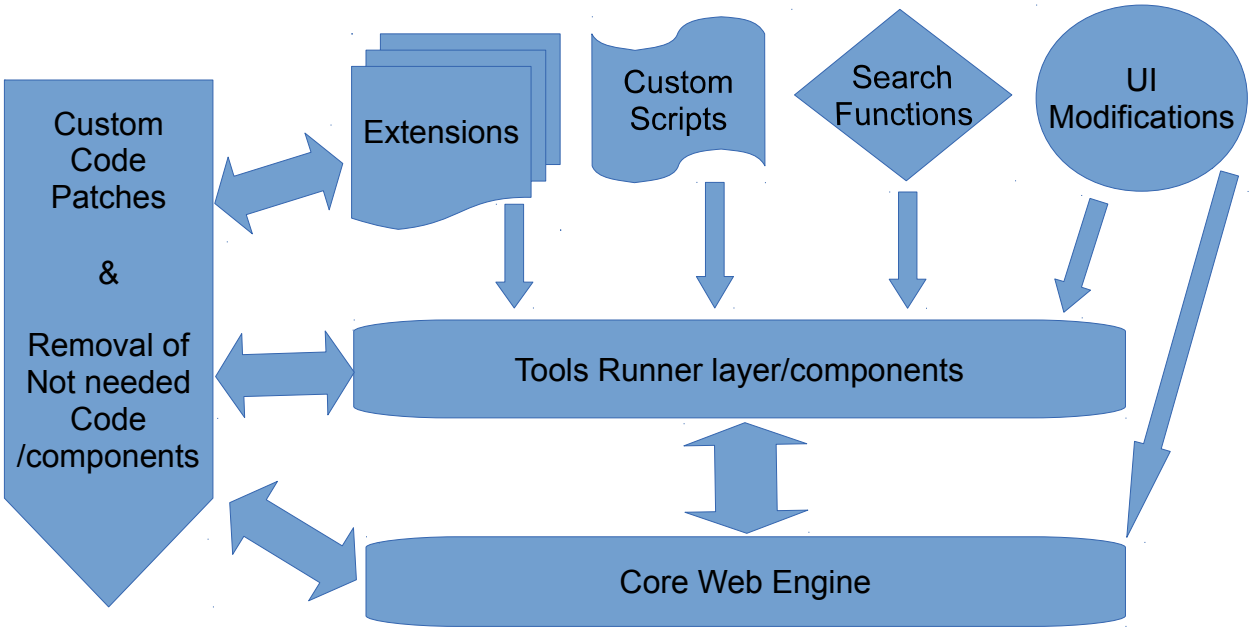


Figure 1: Architecture of HconSTF

It follows a strict design guidelines for the development of the framework which states,

- Give maximum control and decision making ability to the user of the framework unlike other tools in the market which takes away that and leads to more false positives.
- Simple and resourceful tool for web application penetration testing which provides features to get things done easily and also provides learning resources to expand knowledge.
- Provide known and familiar user experience.

1.3 Different Editions

HconSTF comes in two main editions

- Fire base
- Aqua base

Fire base: its build upon Mozilla's technologies which provides,

- Gecko
- XUL runner
- Tons of add-ons
- Inbuilt web debugging tools
- User Interface freedom
- Totally hacker friendliness

The source code is published under MPL v2 and other OSI licenses.

Aqua base: its build upon Chromium technologies which provides,

- Webkit
- Chromium
- Google chrome add-ons
- Minimal and simple user interface
- Strong alternative to Fire base

The source code is published under BSD license and other OSI licenses.

Having two editions based on two different web clients gives more choices to users, also provides bit-different toolset with different designs at base level.

Chapter 2: Origin of HconSTF

In this chapter we will going to look at little history and inspiration behind HconSTF.

2.1 Inspiration

The initial inspiration for this project came from,

- The talk on 'Pen Testing the Web with Firefox' by Michael 'theprez98' Schearer & John 'Dakahuna' Fulmer at last HOPE 2008
- This kind of project came into existence from YGN Group named as hackerfox in Dec 2007

Both of this are core ideas behind HconSTF but they were just a browser technology with some add-ons and was lacking more detailed approach to make it more useful. HconSTF is an effort to expand and build a comprehensive toolset for web application penetration testing based on this ideas.

2.2 Initial Release

The first release version 0.1 was just the ideas from the inspiration with few modifications and was only available to a small set of users who were my students for my security course which i was teaching at a local college. Version 0.2 added more user interface customization and used portableapps as launcher. Version 0.3 based on Firefox version 3.6.17 was first publicly released on June 2011.

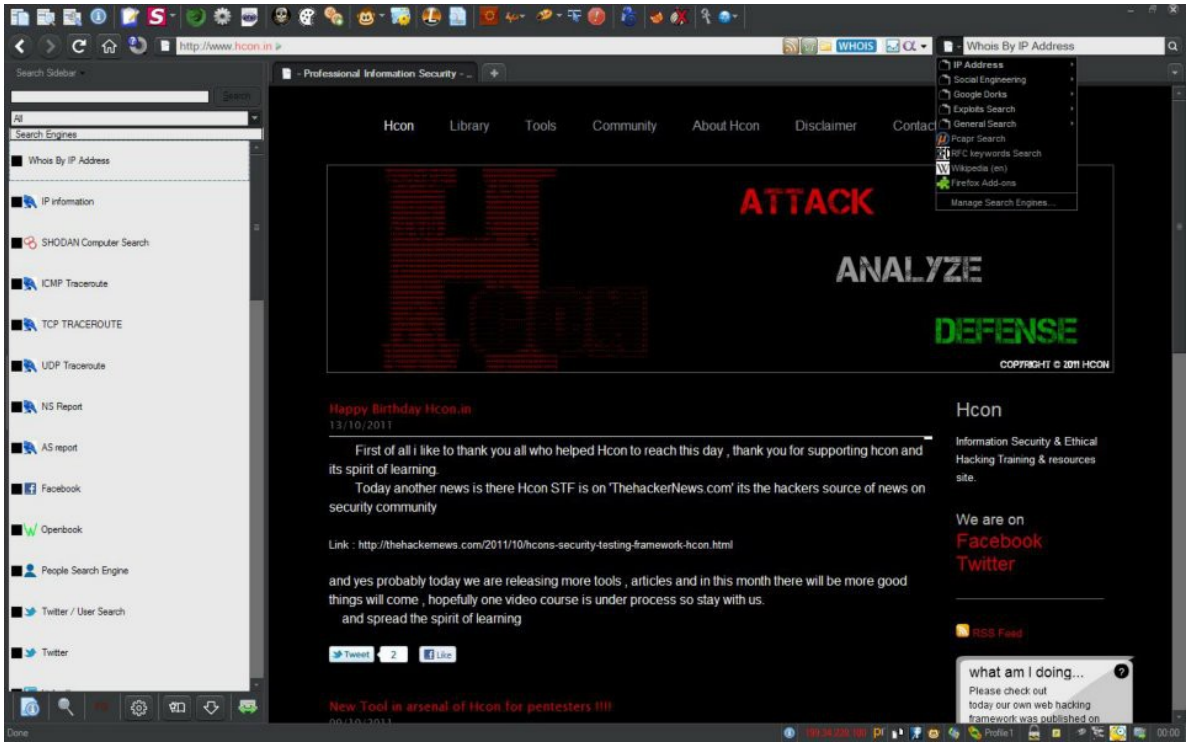

Hcon
Library
Tools
Community
About Hcon
Disclaimer
ATTACK
ANALYZE
DEFENSE
COPYRIGHT © 2011 HCON
Happy Birthday Hcon.in
13/10/2011
First of all i like to thank you all who helped Hcon to reach this day , thank you for supporting hcon and its spirit of learning.
Today another news is there Hcon STF is on 'ThehackerNews.com' its the hackers source of news on security community
Link : http://thehackernews.com/2011/10/hcons-security-testing-framework-hcon.html
and yes probably today we are releasing more tools , articles and in this month there will be more good things will come , hopefully one video course is under process so stay with us.
and spread the spirit of learning
New Tool in arsenal of Hcon for pentesters !!!!
Hcon
Information Security & Ethical Hacking Training & resources site.
We are on
Facebook
Twitter
what am I doing...

Figure 2: HconSTF version 0.3

2.3 First Public Release

This release HconSTF v0.3 was called Hfox (hacker+firefox) initially had ~2000 downloads in just few time and with some response from the security community for improvements as they wanted to see more like this, so as a result the name changed to Hcon Security Testing Framework and lots of changes and improvements had made into 0.4 codename 'Freedom'.

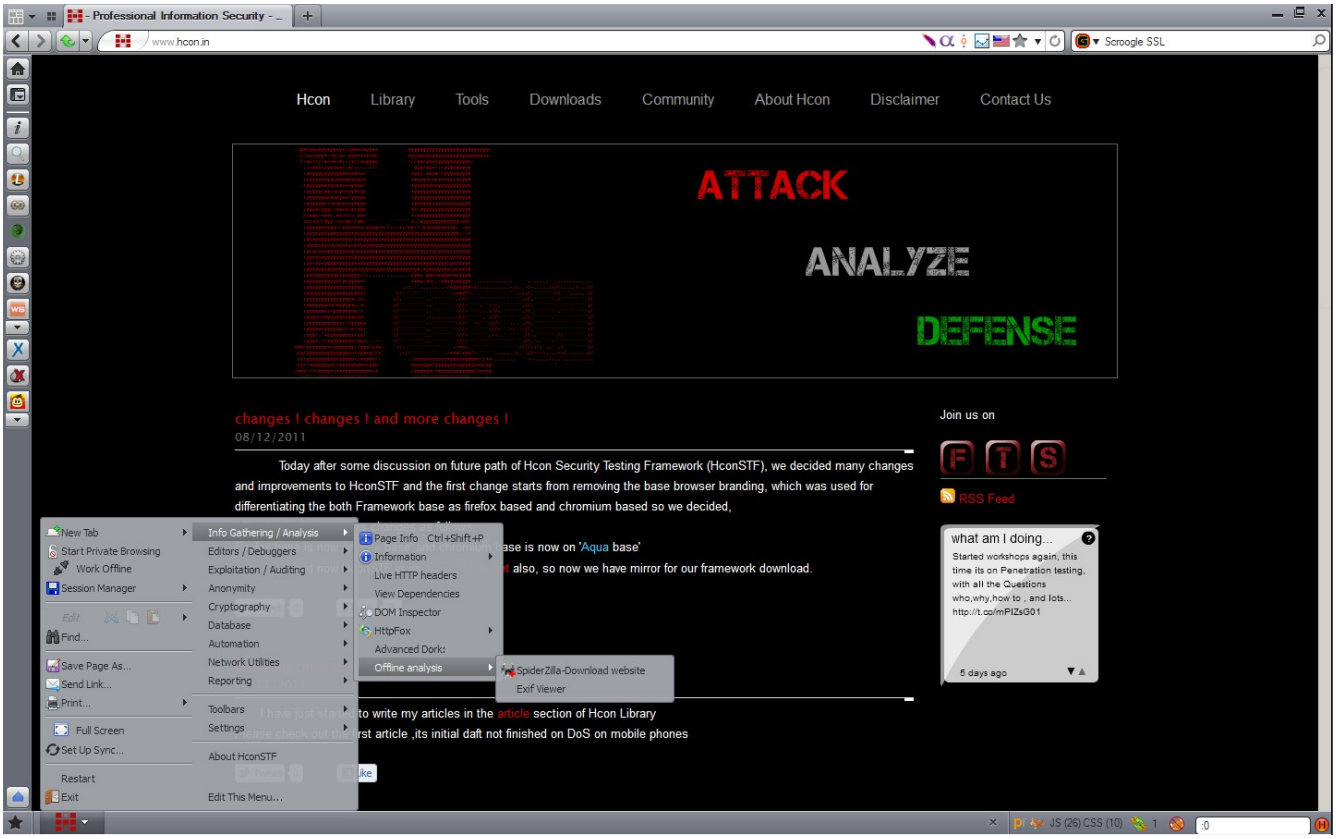


Figure 3: HconSTF version 0.4 codename 'Freedom'

Chapter 3: Getting Started with HconSTF

In this chapter we will acquire the things to actually get up and running with HconSTF and how to configure its basic settings.

3.1 Prerequisites

Recommended system requirements for HconSTF

- Operating System:
  - Microsoft Windows XP SP2 or higher
  - Microsoft Windows vista
  - Microsoft Windows 7
  - Microsoft Windows 8 and 8.1
  - All major Linux distributions including kali, backtrack, backbox
- Hardware:
  - CPU: 1GHz x86 and x64 architecture
  - RAM: 1 GB minimum
  - Hard Disk Space: 150 MB

Note: *the software requirements are same as firefox.*

3.2 Downloading HconSTF

For downloading HconSTF just visit the url: http://www.hcon.in/downloads.html download as per our operating system as current version is available for Windows and Linux for both x86 and x64 architectures.

Current version is available as portable application which doesn't need to install into our operating system but for using it just download and extract it anywhere on hard disk or other memory storage device like memory card, USB pendrives, external hard disk and run the launcher.

Warning: *There are many fake binaries of HconSTF floating around on torrent and other rouge download sites so only download from the official site which is http://www.hcon.in/*

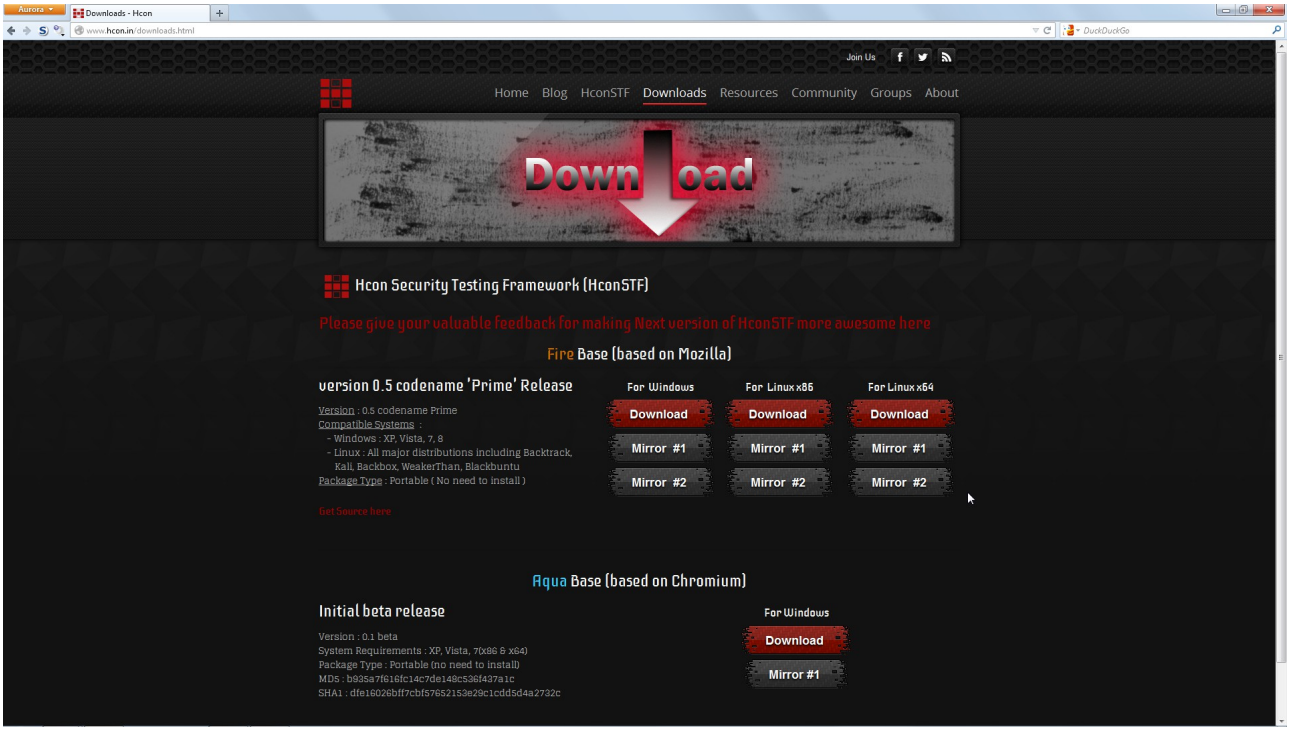


Figure 4: Official downloads page for HconSTF

3.3 Setting all up

After downloading just extract the packages of HconSTF and execute the launcher

For Windows:

Double click on HconSTF_v0.5_Prime.exe

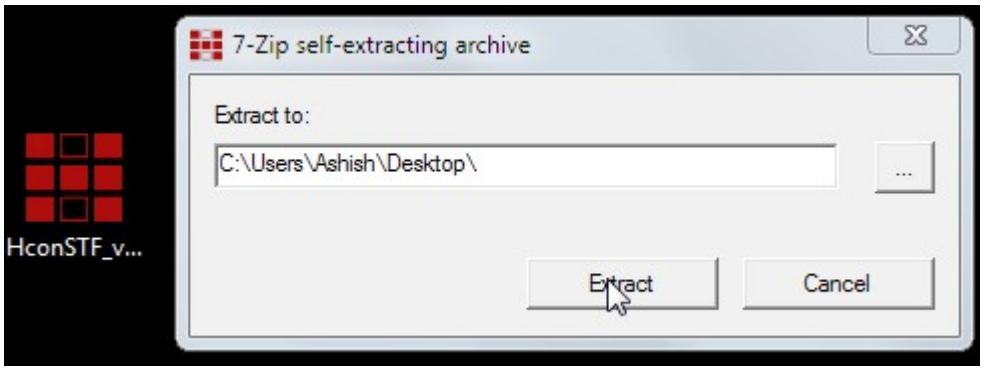


Figure 5: Extracting downloaded windows package

Open HconSTFportable directory and run HconSTFportable.exe as Administrator

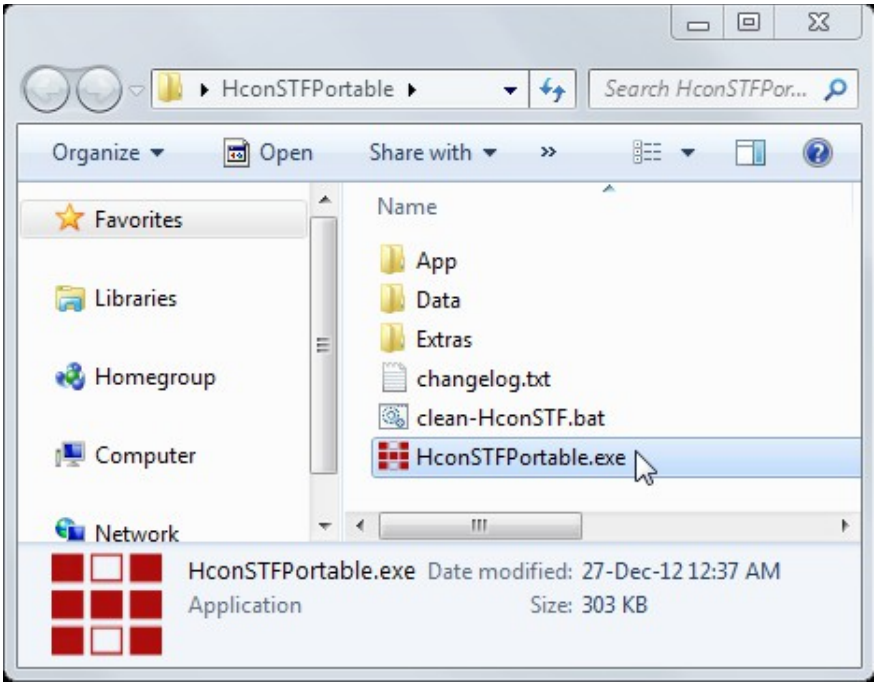


Figure 6: HconSTF main directory

For Linux:

Open Terminal window and navigate to the directory where HconSTF is downloaded and run

```
tar -xvf ./HconSTF_v0.5_Linux_x86.tar.bz2
```

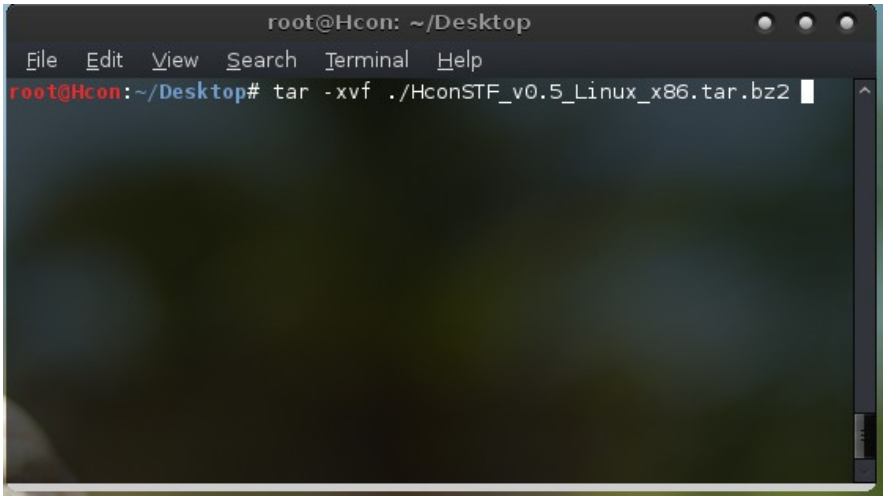


Figure 7: Extracting downloaded linux package

Now navigate into HconSTF directory by running cd HconSTF

Give executable permissions to HconSTF launcher

`sudo chmod +x ./HconSTF` (for non root user)

`chmod +x ./HconSTF` (for root user)

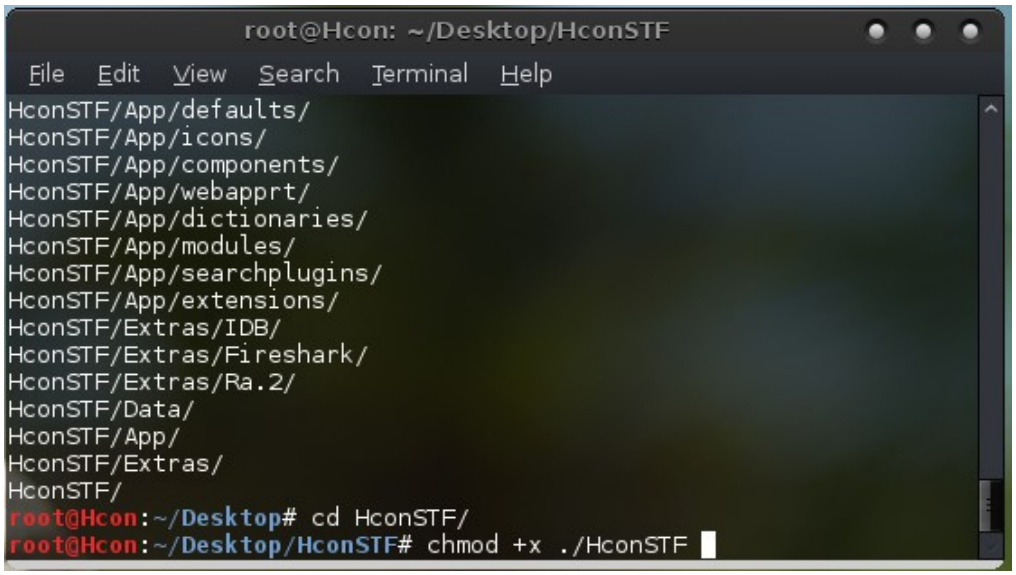


Figure 8: Giving executable permissions to HconSTF launcher

For starting HconSTF type and execute

`sudo ./HconSTF` (for non root user)

`./HconSTF` (for root user)

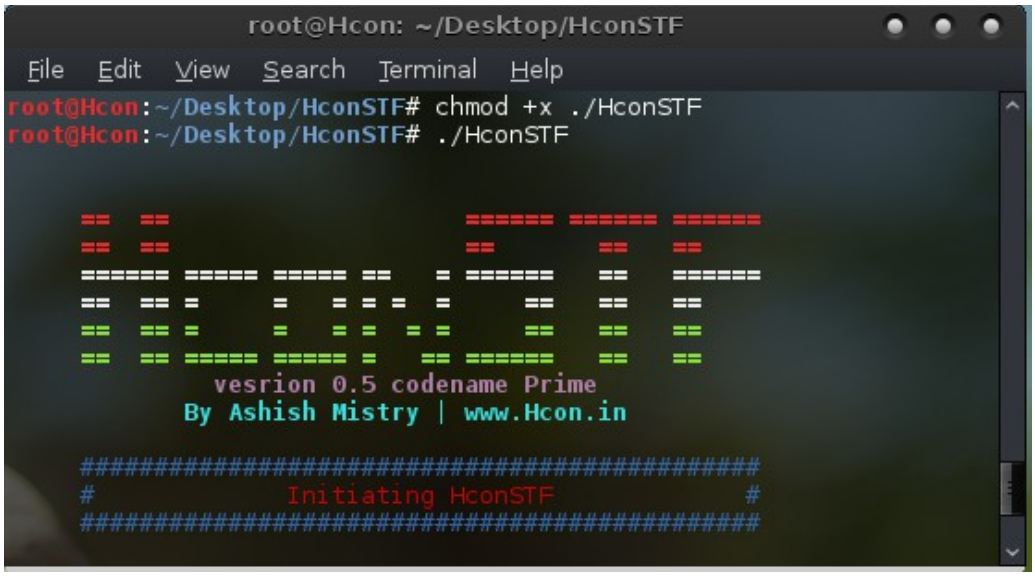


Figure 9: Launching HconSTF under linux

Note: *Don't close the terminal window after graphical window is opened.*

3.4 Familiarization with User Interface

User interface of HconSTF is very intuitive and designed with focusing on accessibility and simplicity. Its an OS shell like interface with bottom panel, consists of menu in down left and status icons in down right area.

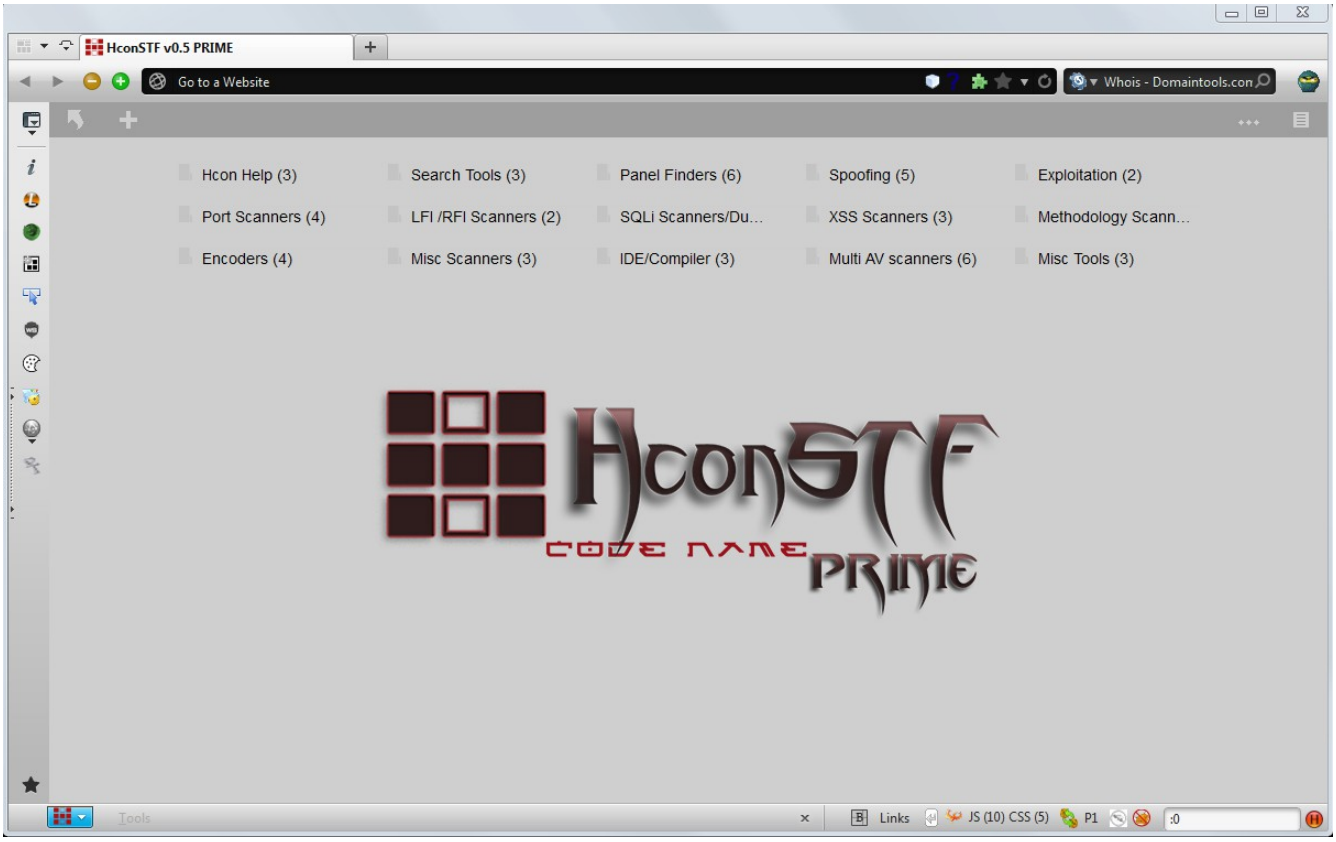


Figure 10: Default start window of HconSTF

Note: *This is the default user interface which can be easily customizable to suite our needs.*

Lets have a closer look into HconSTF user interface and get familiar with it.

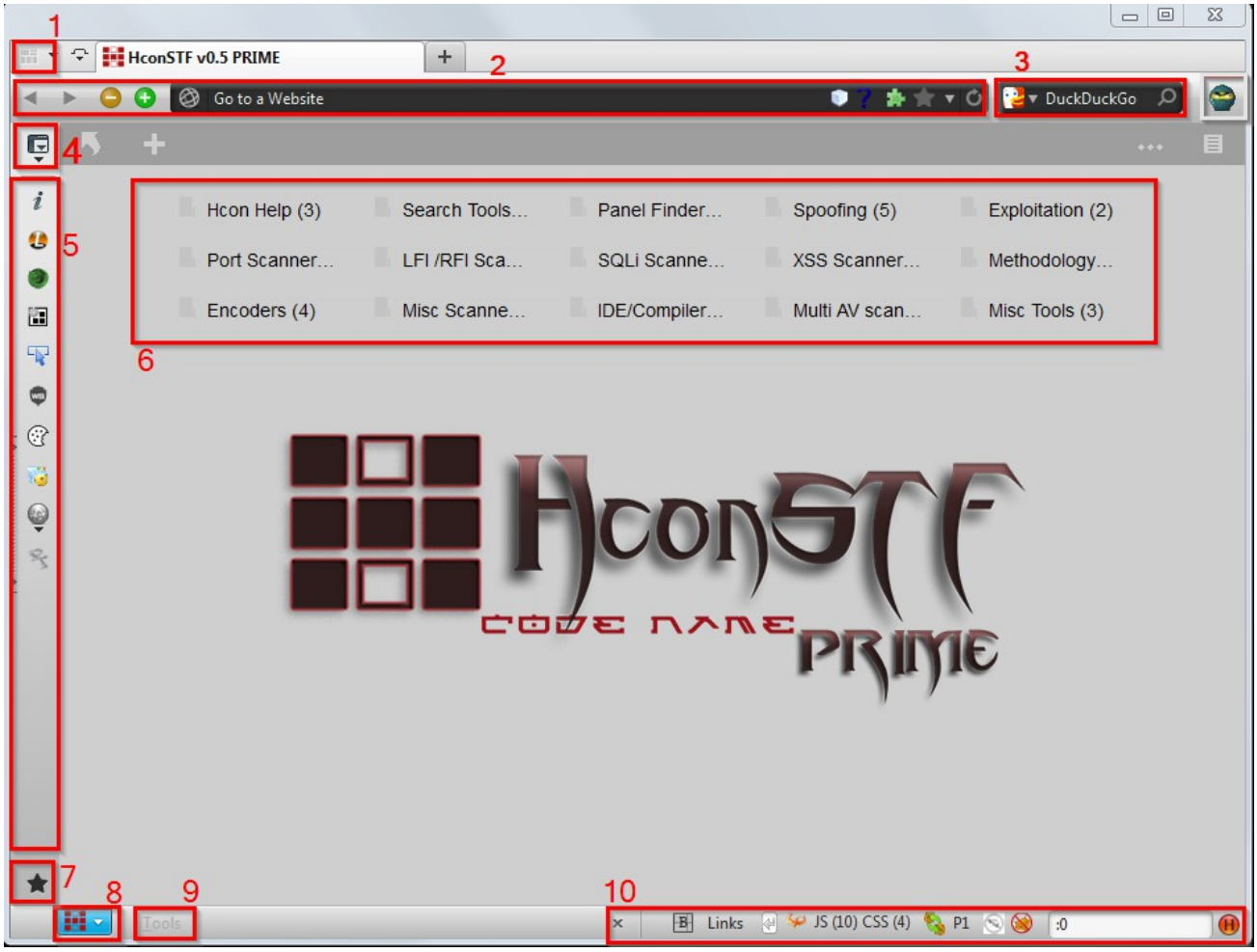


Figure 11: Highlighted different user interface elements

1. Tile tabs button – Arranges multiple tabs into tiles in one window
2. Url address bar – Navigate through web address
3. Search Aggregator – For searching on everything
4. All sidebar panels button – Accessing and opening different sidebars
5. Sidebar – simple launcher panel with tool buttons
6. WebUI – Categorized online tools
7. Hackery Hybrid/Bookmarks button – Access all learning resources web links
8. H menu button – Main menu with categorized built-in tools
9. All tools menu button – All built in tools without categorization
10. Status bar – Access quick tools and see notifications

Above elements in action:

Figure 12: Tabs in single window as vertical tiles

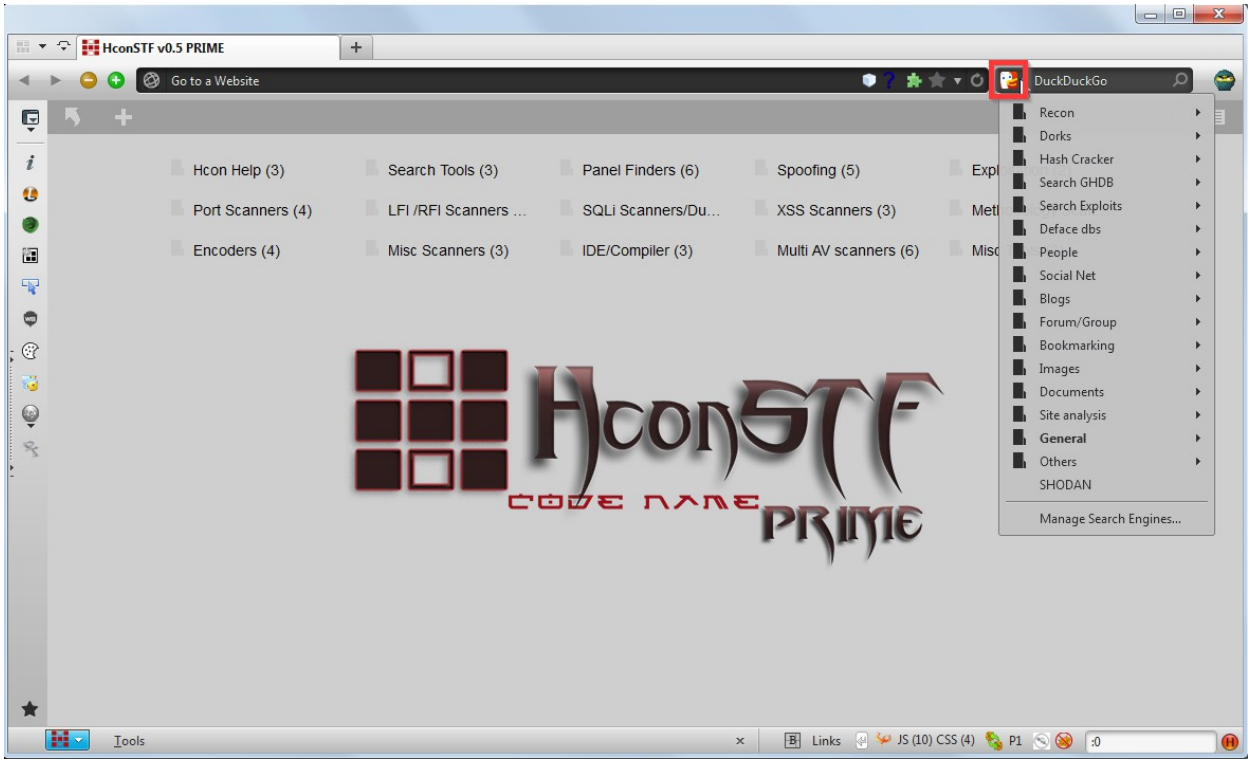


Figure 13: Opening search aggregator

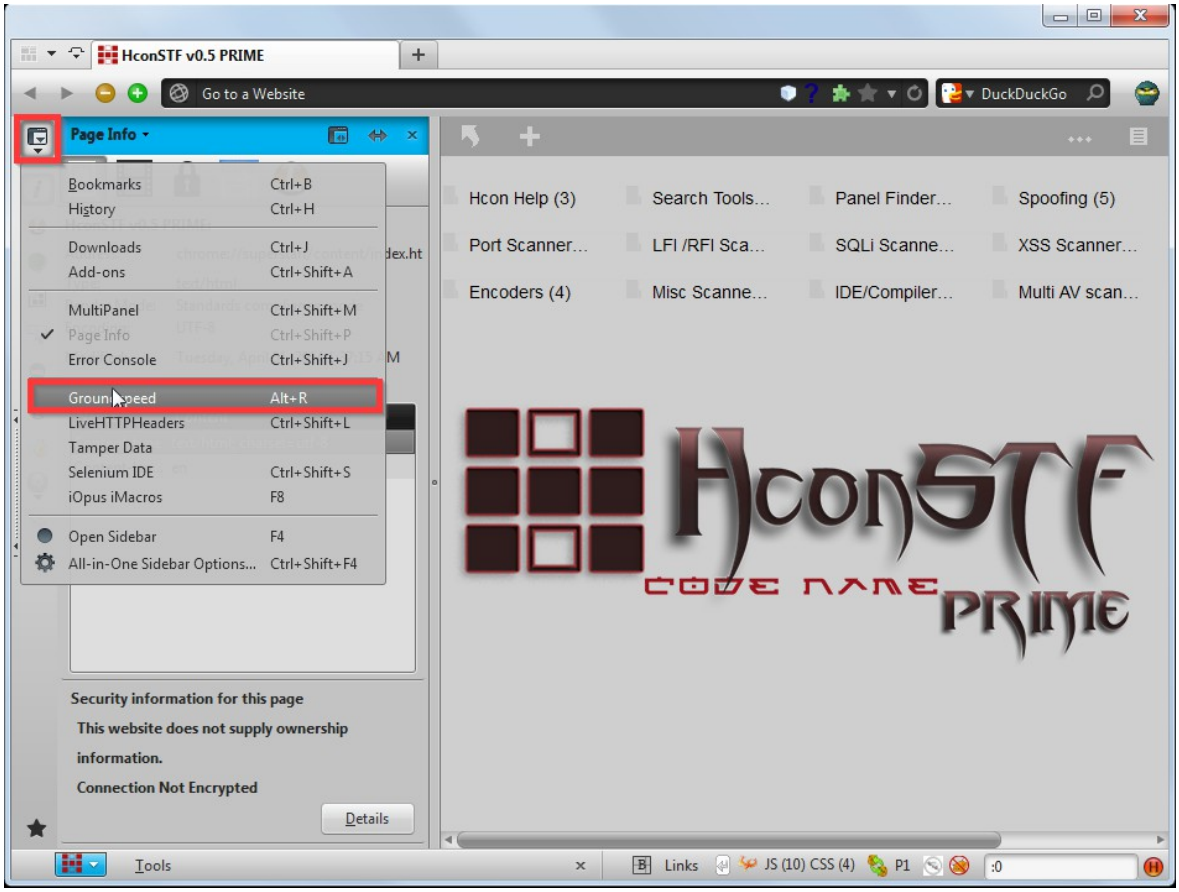


Figure 14: Accessing all sidebar panels

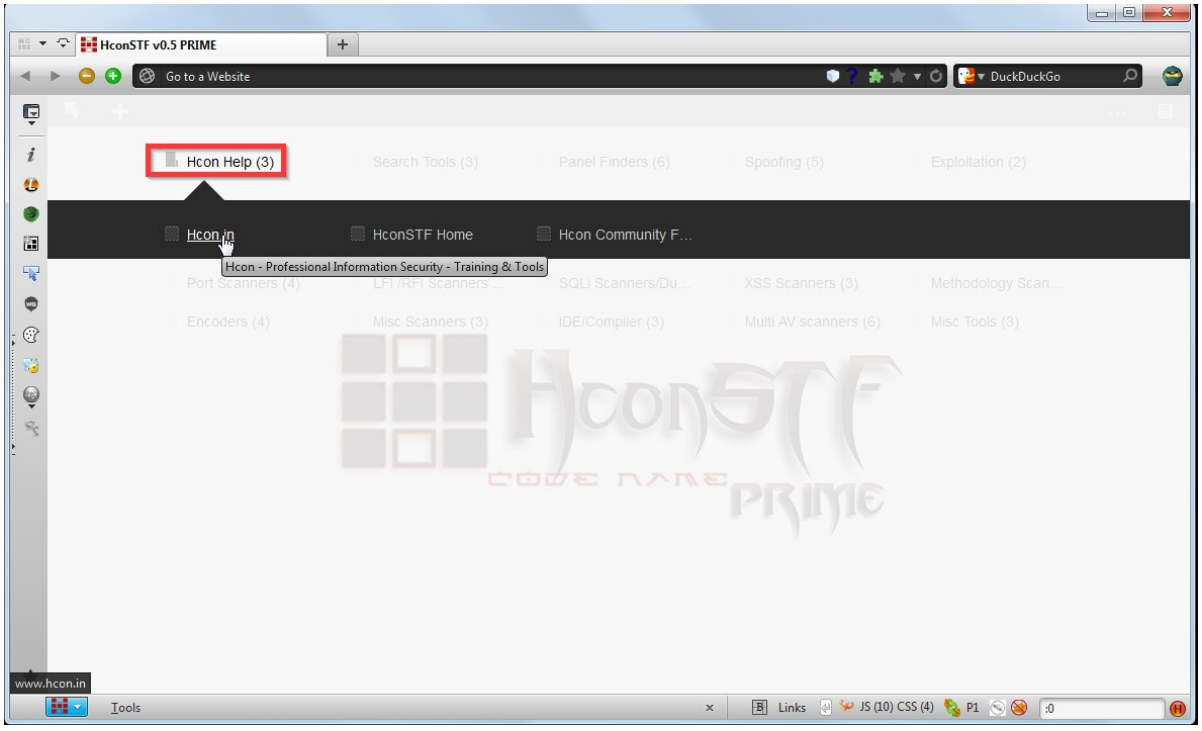


Figure 15: Accessing individual tools from WebUI

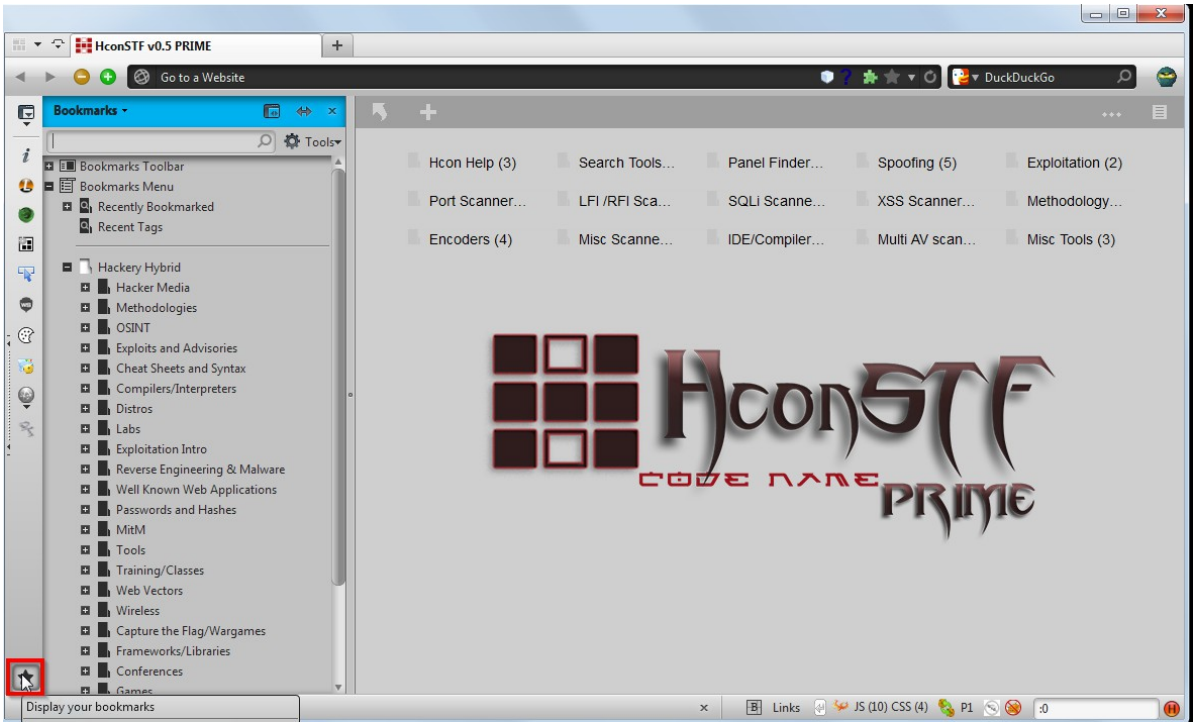


Figure 16: Plethora of learning links in Hackery Hybrid

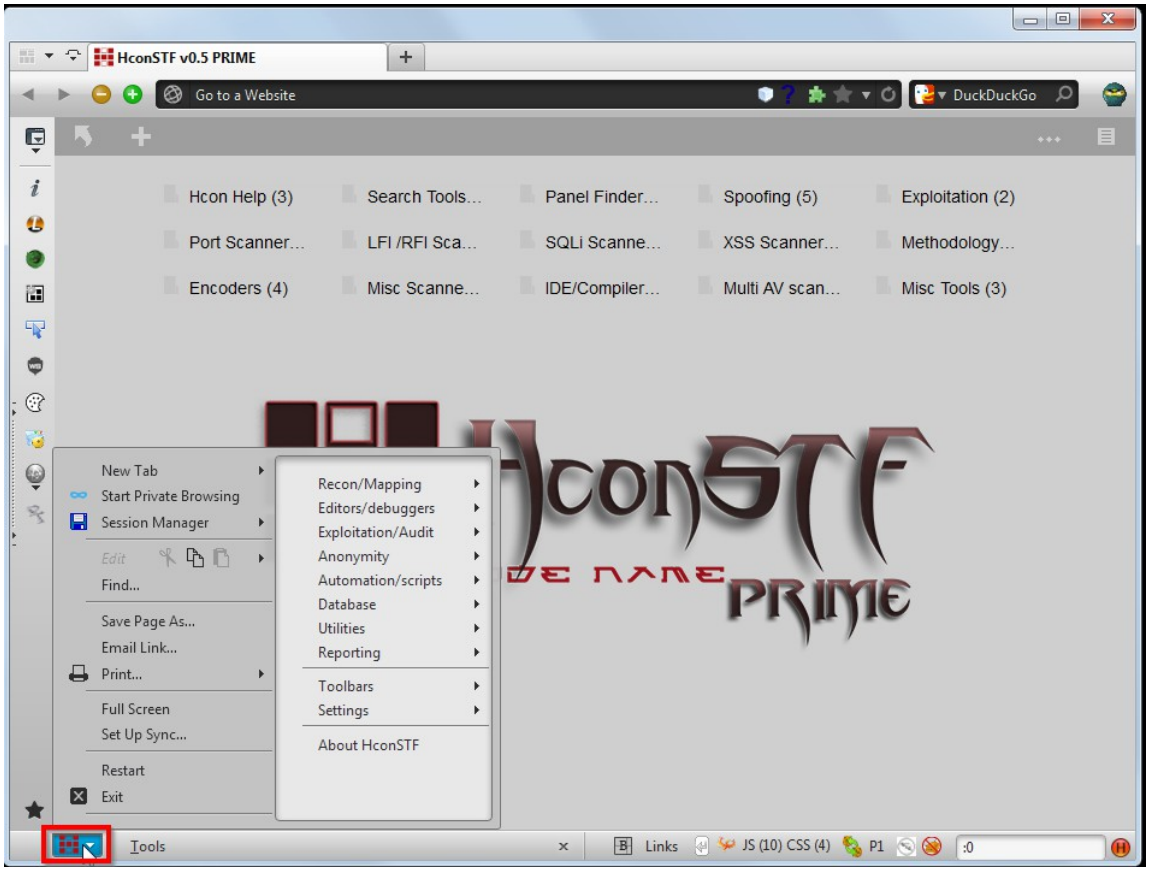


Figure 17: Hmenu - categorized main menu

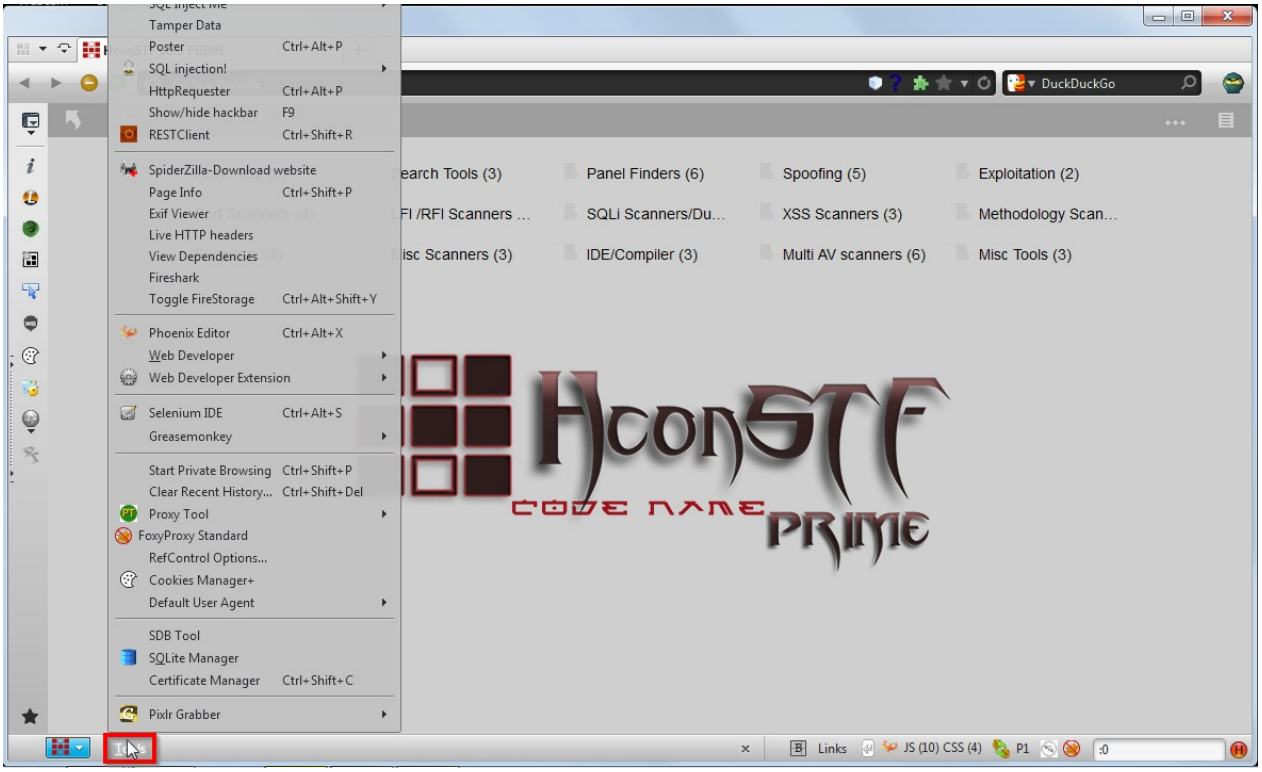


Figure 18: All tools in a single menu

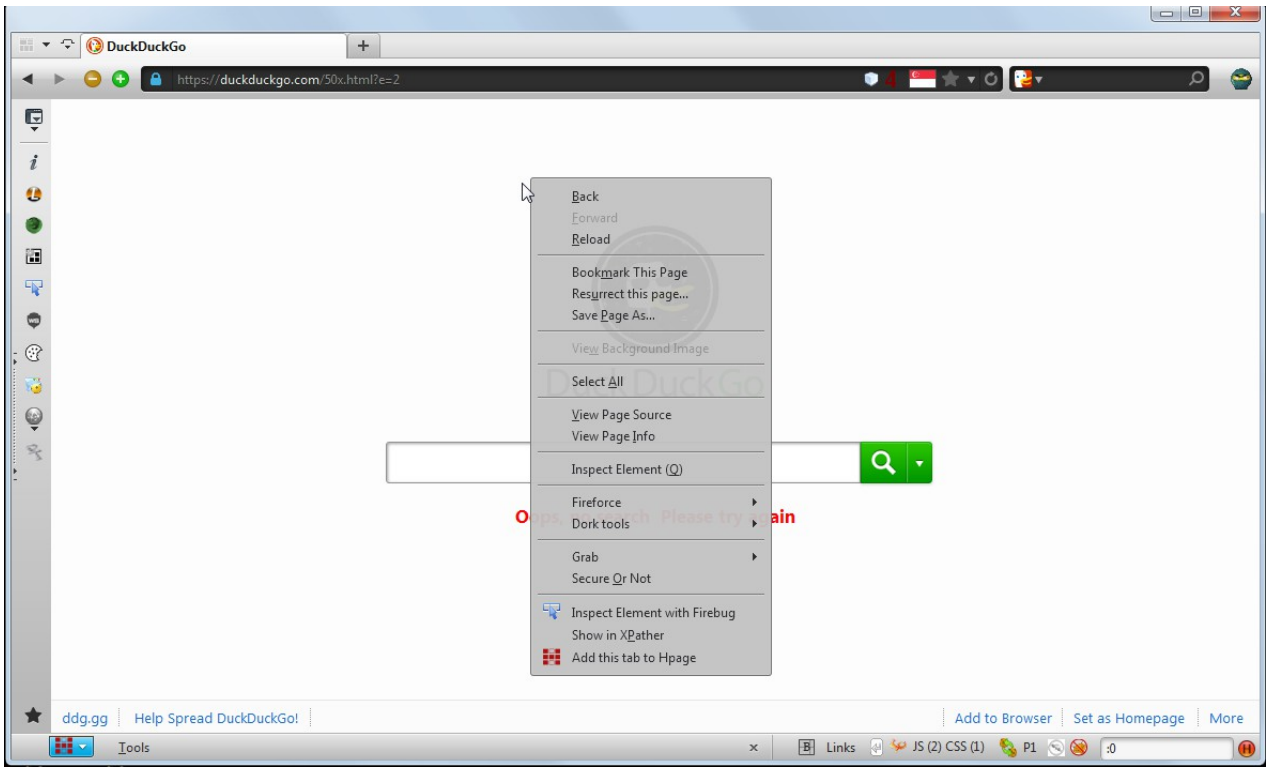


Figure 19: Content aware context menu

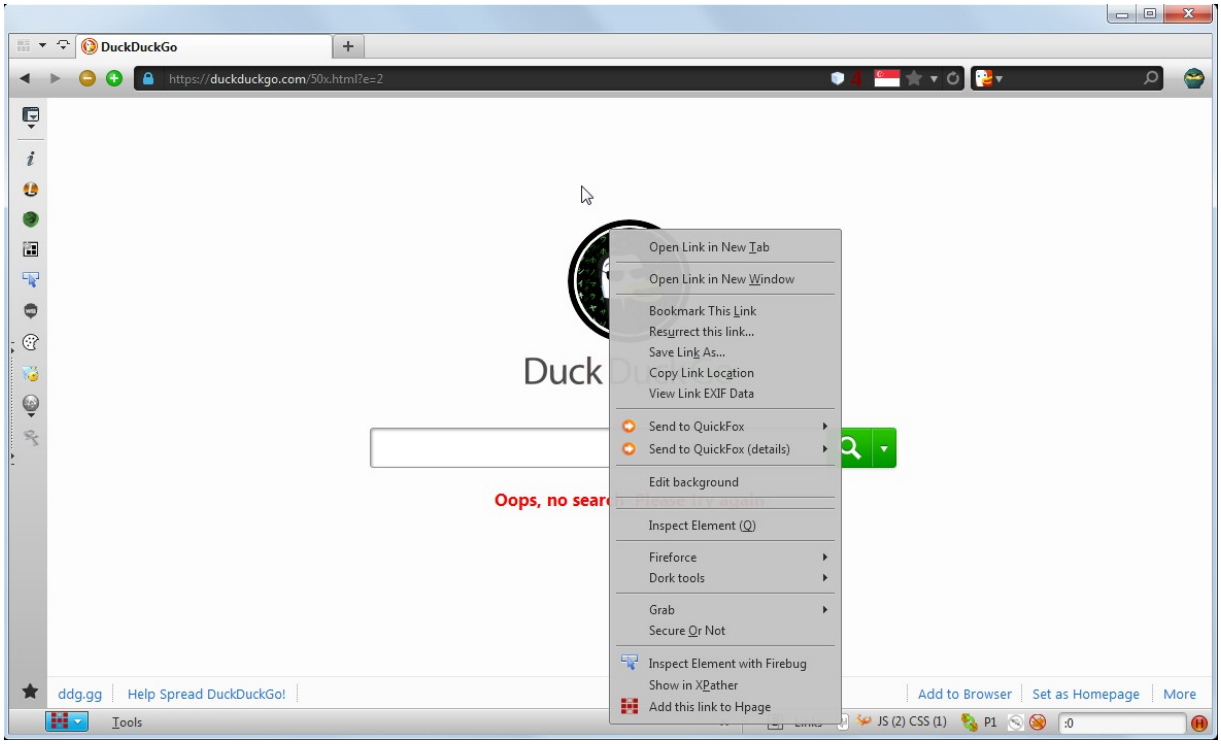


Figure 20: Context menu for images

3.5 Customizing Preferences

In general HconSTF comes preconfigured and it is ready to use once we extract it but we can still configure a lot of options to suite our needs. all the settings are at Hmenu → Settings

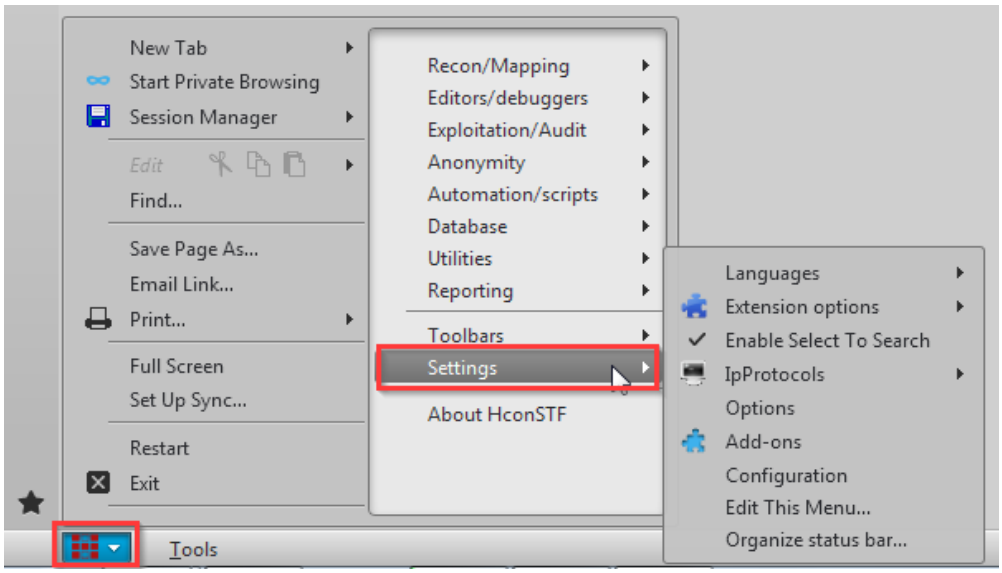


Figure 21: All settings menu

We can configure most of the framework from this menu only, including tools setup, changing language, behavior, advanced tweaking, user interface customization and more.

Changing Language

The default HconSTF packages are only in english language however HconSTF has partial multilingual support, meaning that most of its user interface will be translated into our chosen language. For changing language download additional language pack add-ons (.xpi) according to our language-region code and install it by dragging and dropping it over HconSTF window, after restarting HconSTF our installed language will appear in language settings.

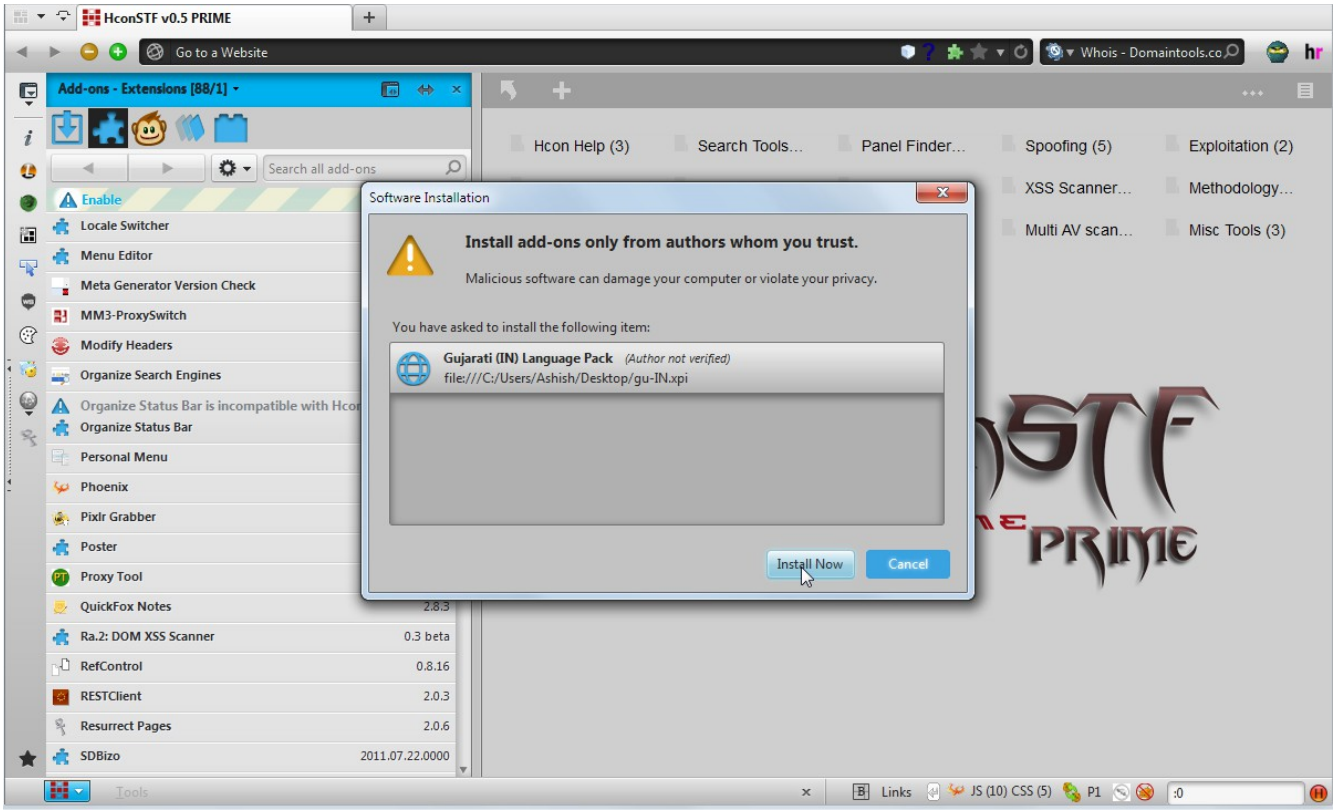


Figure 22: Installing language pack

Language pack download locations:

- For windows: ftp://ftp.mozilla.org/pub/mozilla.org/firefox/releases/17.0.1/win32/xpi/
- For linux x32: ftp://ftp.mozilla.org/pub/mozilla.org/firefox/releases/17.0.1/linux-i686/xpi/
- For linux x64: ftp://ftp.mozilla.org/pub/mozilla.org/firefox/releases/17.0.1/linux-x86_64/xpi/

We can switch between languages from: Hmenu → Settings → Languages and select the language we want to apply and restart HconSTF

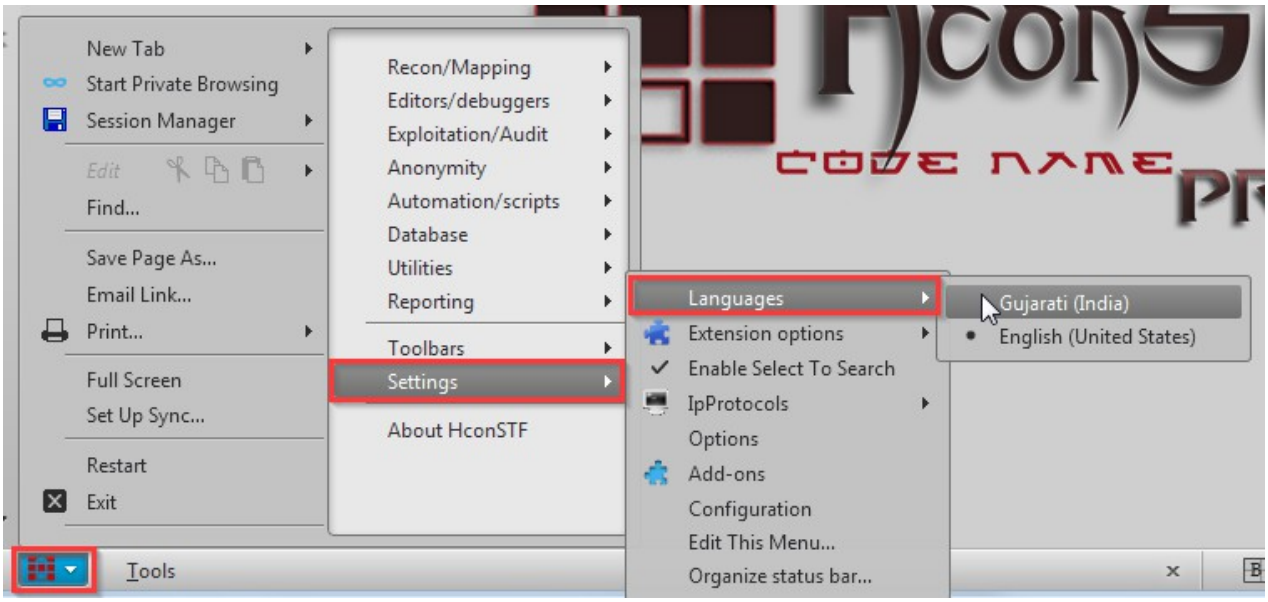


Figure 23: Changing user interface language

Changing individual tool settings

There are ton of tools built into HconSTF and we can configure each to our needs from:

Hmenu → Settings → Extension Options

Select the tool we want to configure, it will present us with available options for that tool.

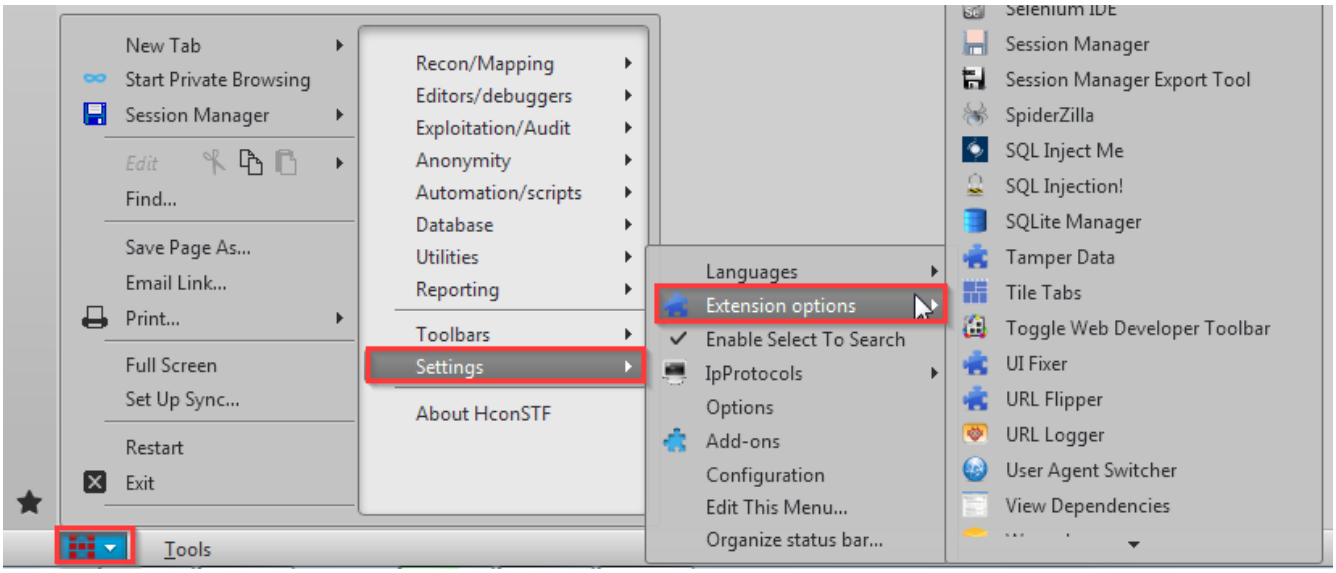


Figure 24: Customize individual tools settings

Disable selected text to search aggregator

Its a unique feature which is enabled by default, basically it copy the text we select on the web page and paste it automatically into search aggregator then we just have to select our search engine and it will search that text in a new tab.

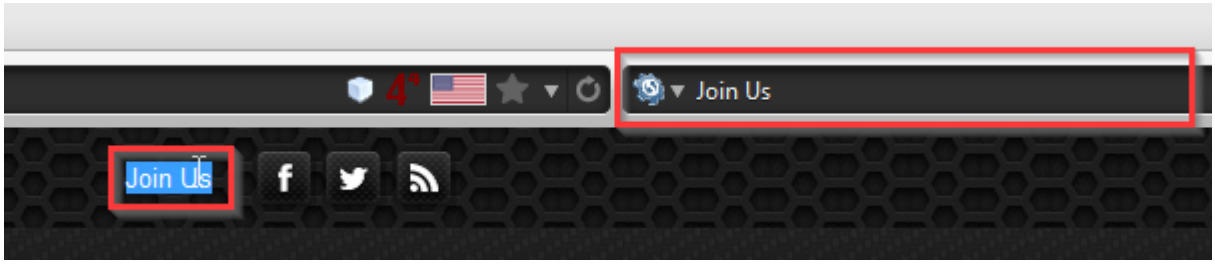


Figure 25: Auto copy text into search aggregator

Disabling or enabling it in a single click from: Hmenu → Settings → Enable Select to search

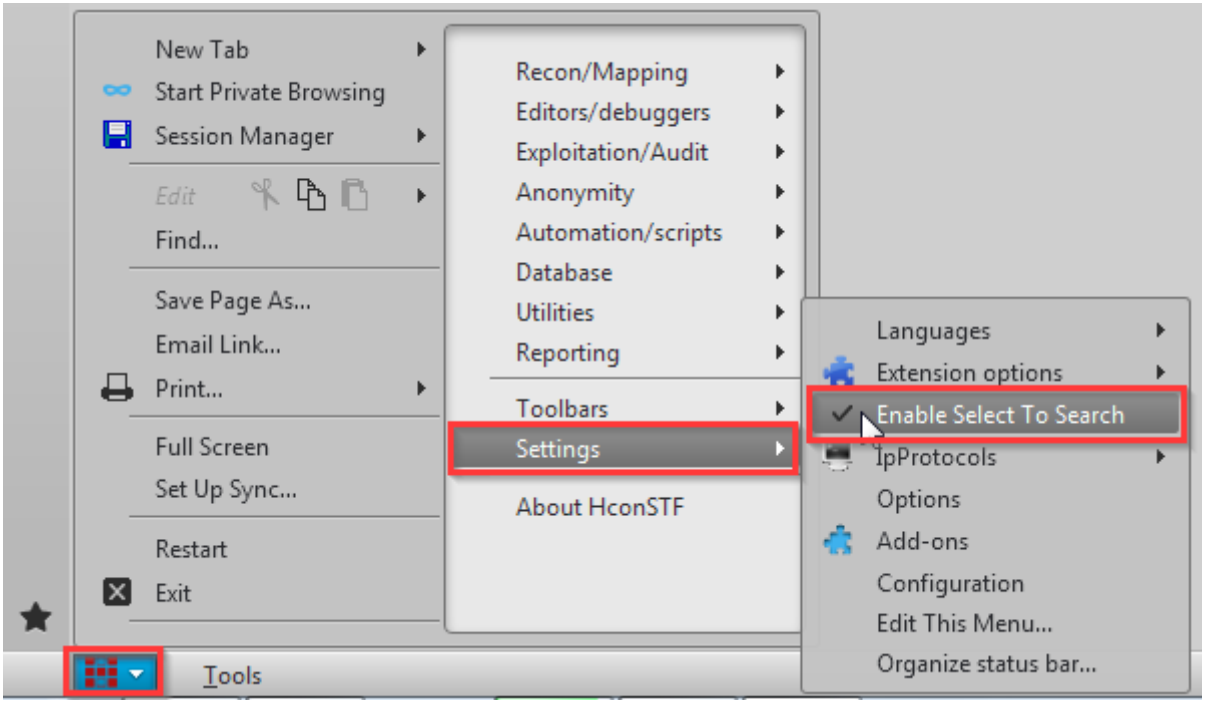


Figure 26: Auto copy text to search aggregator settings

Configuring external tools

We can attach and configure many external tools in HconSTF and all the tools can take IP address as input argument and then run on that IP address with configured options.

We can access this settings from: Hmenu → Settings → IPprotocols

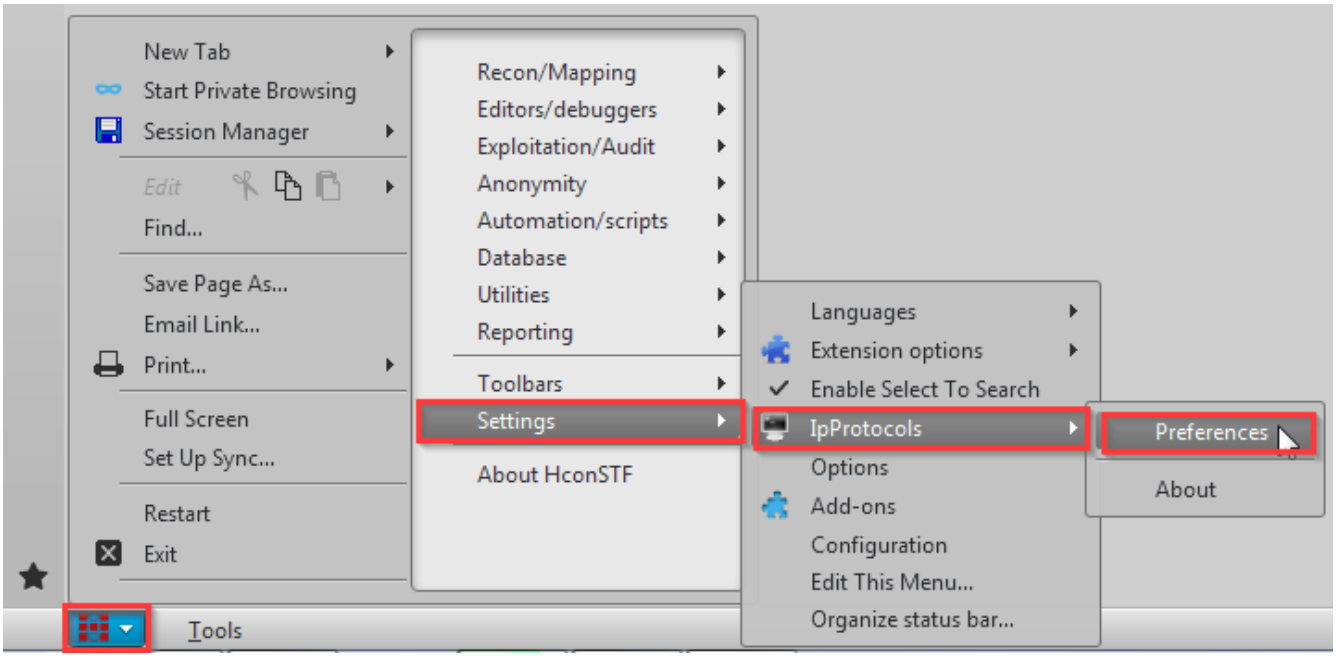


Figure 27: External tools settings

We will see how to setup this tools with HconSTF in Chapter 8.1

Changing general settings

We can configure general options like default download location, network settings, crypto options etc. from: Hmenu → Settings → Options

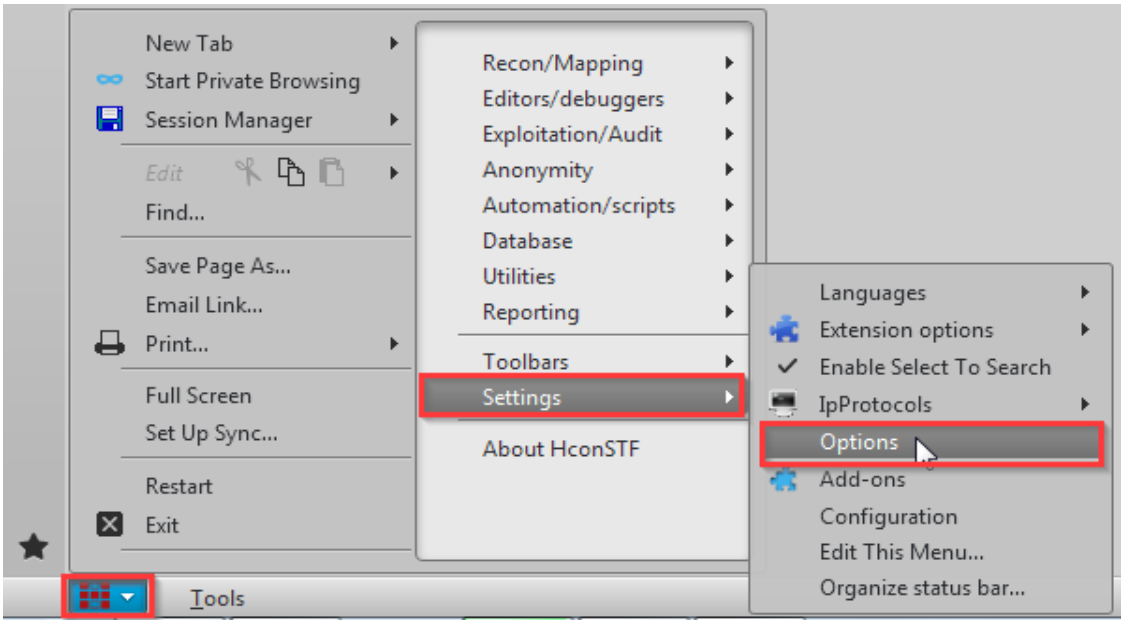


Figure 28: General options menu

Default landing page is set to HconSTF WebUI and also it is recommended not to change it else we will loose access to WebUI and all of its tools.

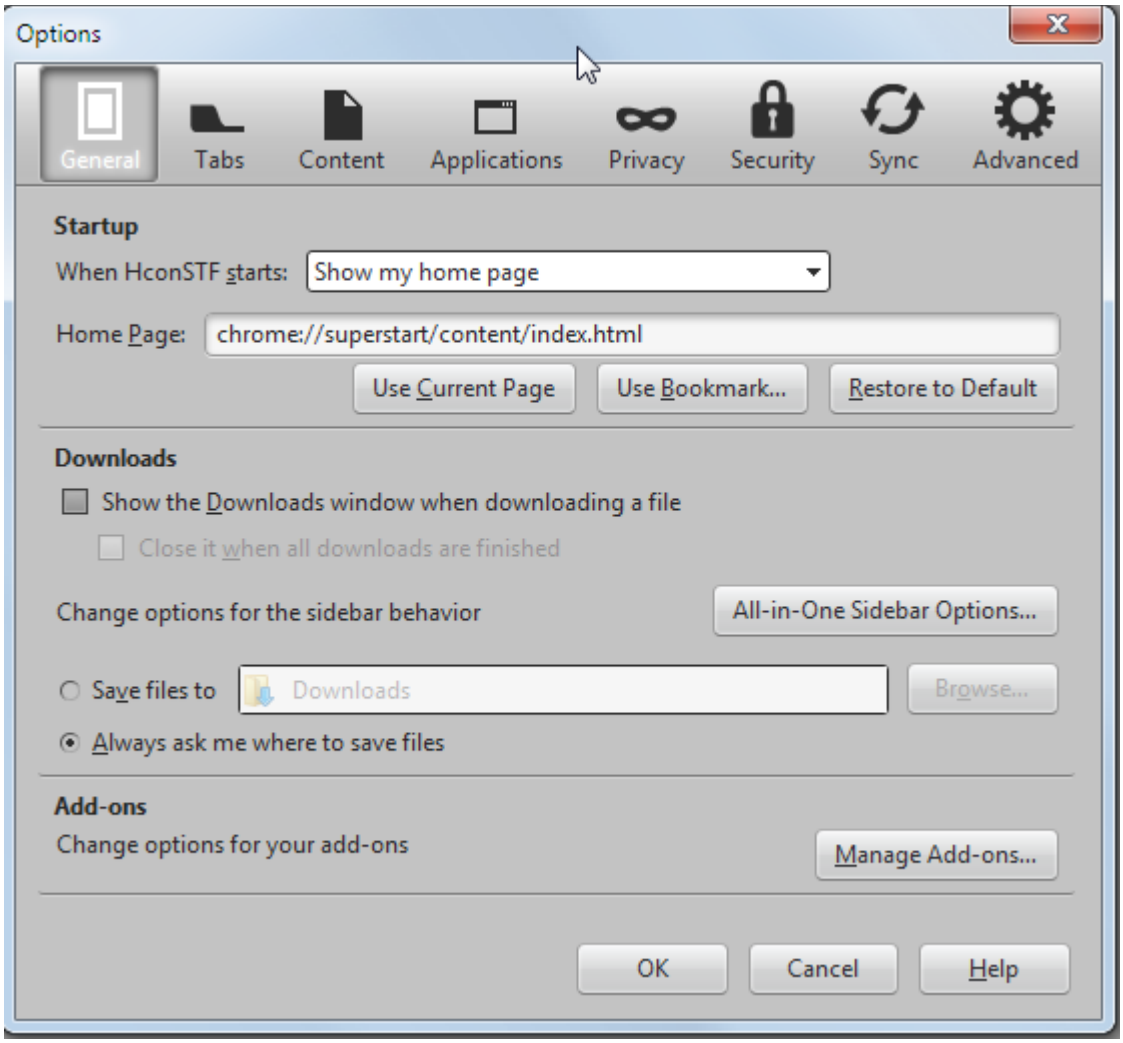


Figure 29: General preferences window

Note:

1. *Auto page redirection is blocked by default and HconSTF will ask permission for this kind of requests, this can be disabled from this menu only.*
2. *Malware protections are disabled by default and it is recommended to keep it like this for web malware analysis else it can be enabled from this menu only.*

Enable / Disable inbuilt tools

Access all the inbuilt tools and we can enable/disable or remove and update it from this menu from: Hmenu → Settings → add-ons

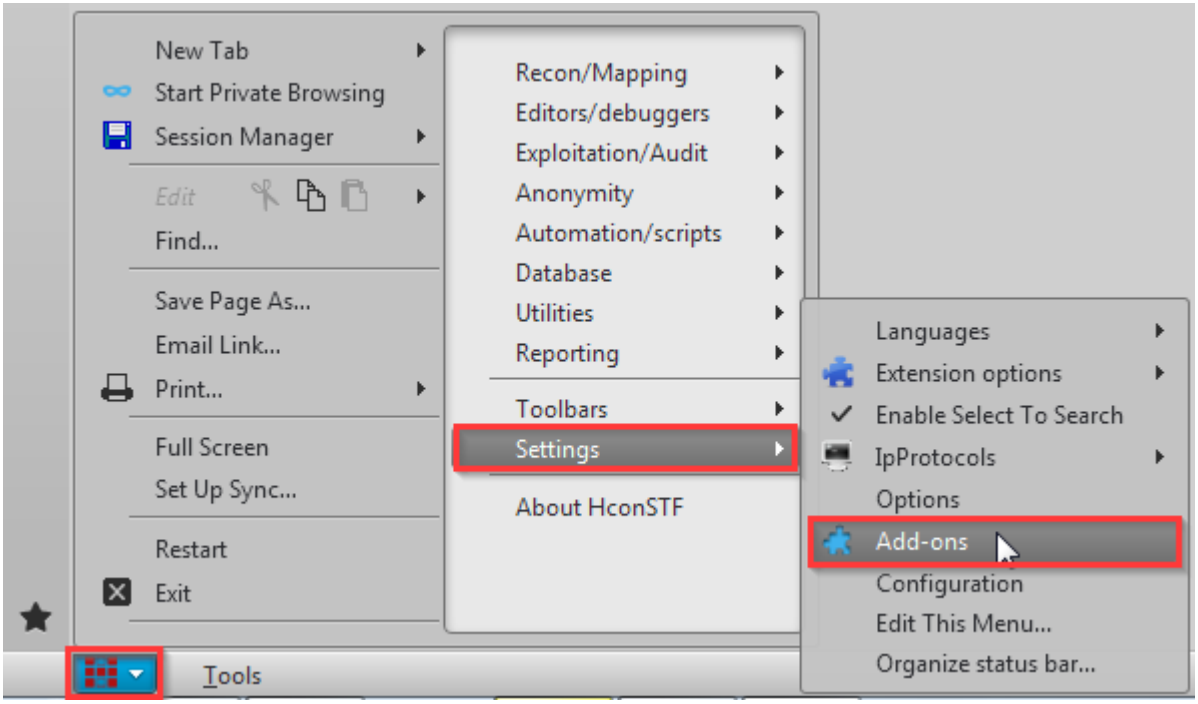


Figure 30: Accessing Individual tools

It will be opened in sidebar, from this it is possible to also access greasemonky scripts settings, change the user interface theme of HconSTF, enable or disable web plugins like flash, silverlight, java etc.

Advanced Tweaking

This menu is only recommended for power users, as this alters entire behavior of the framework, access it from: Hmenu → Settings → configuration

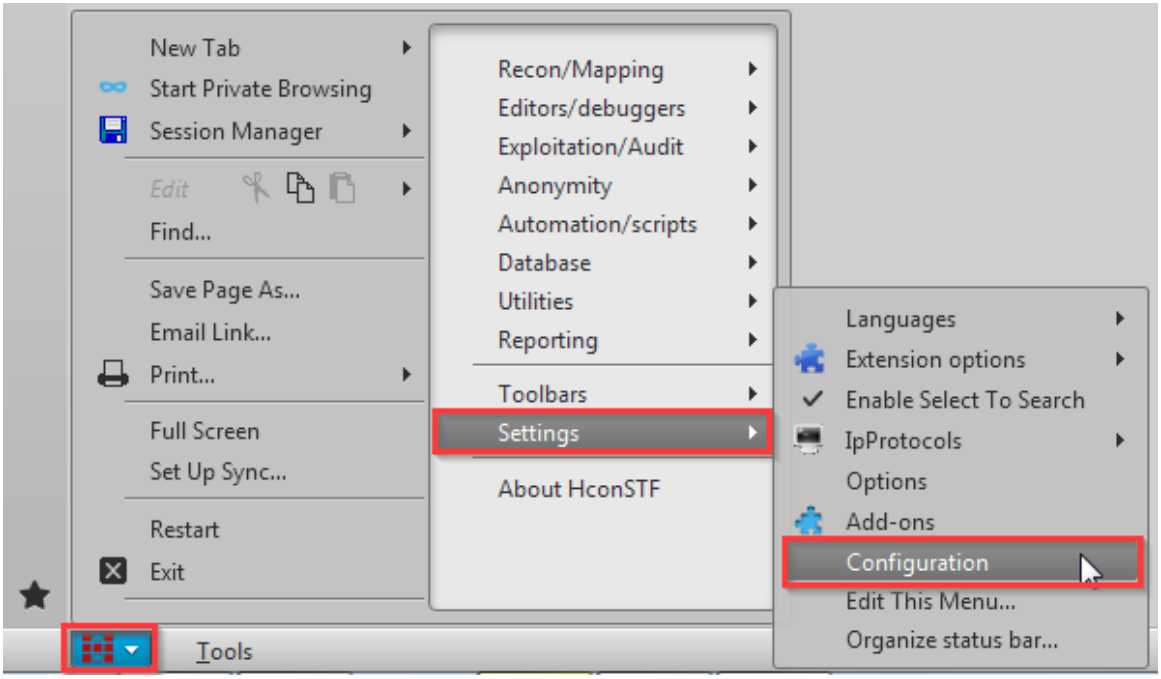


Figure 31: Advanced configuration menu

Tweak different configurations directly from it only if you know what you are doing

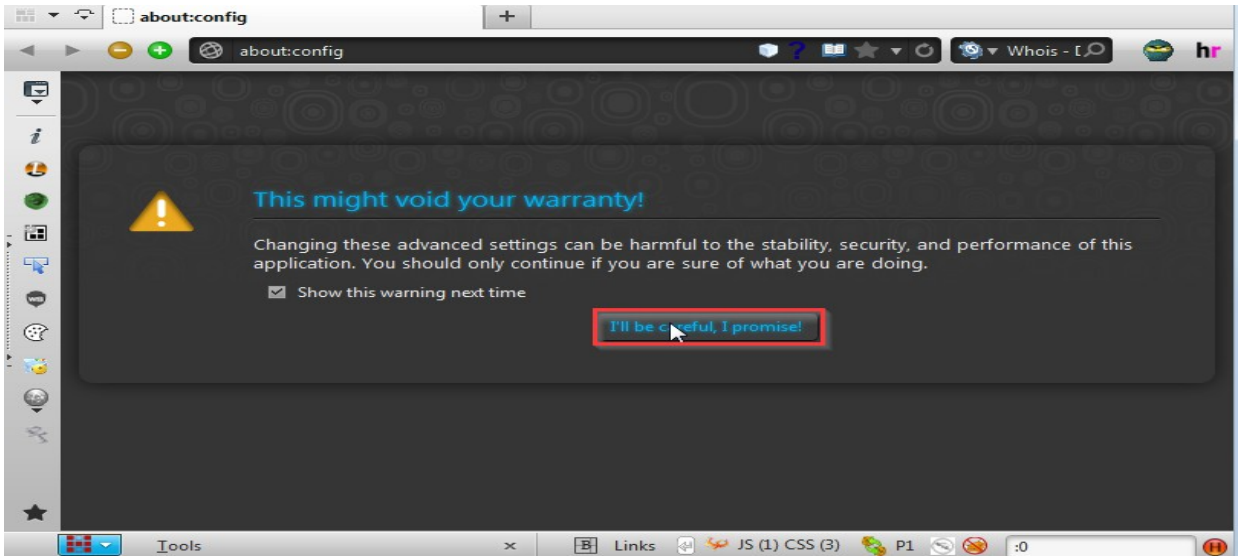

about:config
about:config
Whois - [
This might void your warranty!
Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.
Show this warning next time
I'll be careful, I promise!
Tools
Links
JS (1) CSS (3)
P1

Figure 32: Accept warning and access advanced options

Note: *be very careful when using this configuration as this can cause malfunctioning in HconSTF*

Customizing Hmenu

For customizing Hmenu, open Hmenu editor from: Hmenu → Settings → Edit this menu

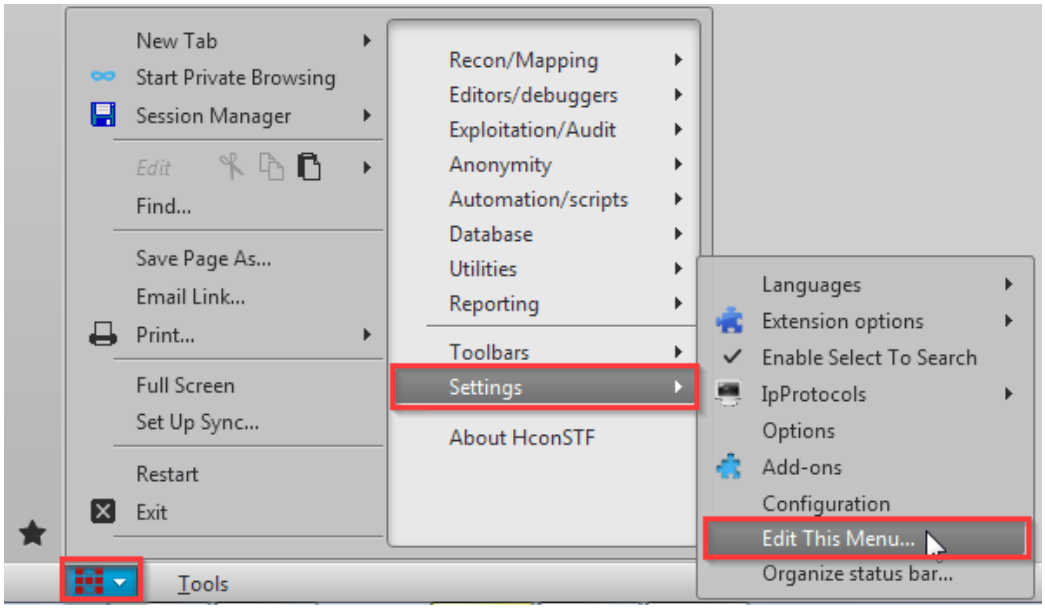


Figure 33: Customizing Hmenu

Using Hmenu editor we can rearrange categories in it and customize individual entries in it easily, we can edit or recreate new menu entries or make new sub menu etc.

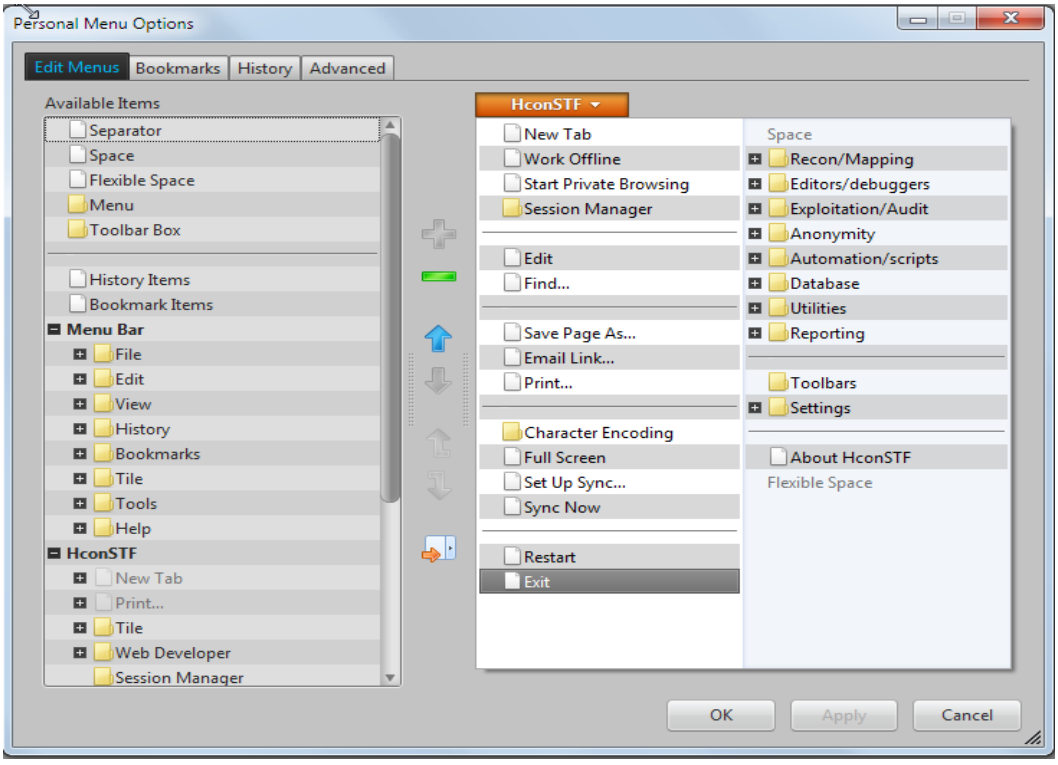


Figure 34: Hmenu editor

Customizing status bar

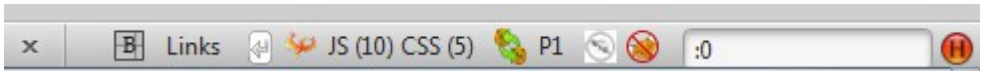


Figure 35: Status bar area

We can customize the status bar area at downright corner of HconSTF with enabling or disabling and rearranging tools and its notifications from: Hmenu → Settings → Organize status bar

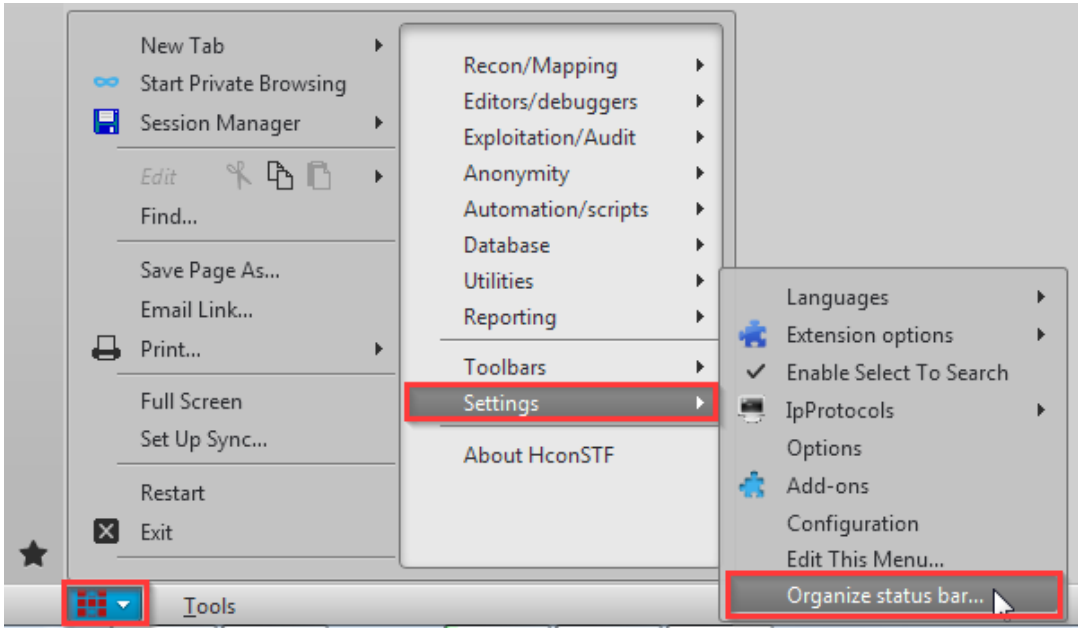


Figure 36: Customize status bar menu

We can rearrange the order of tools which are displayed and enable the default hidden tools.

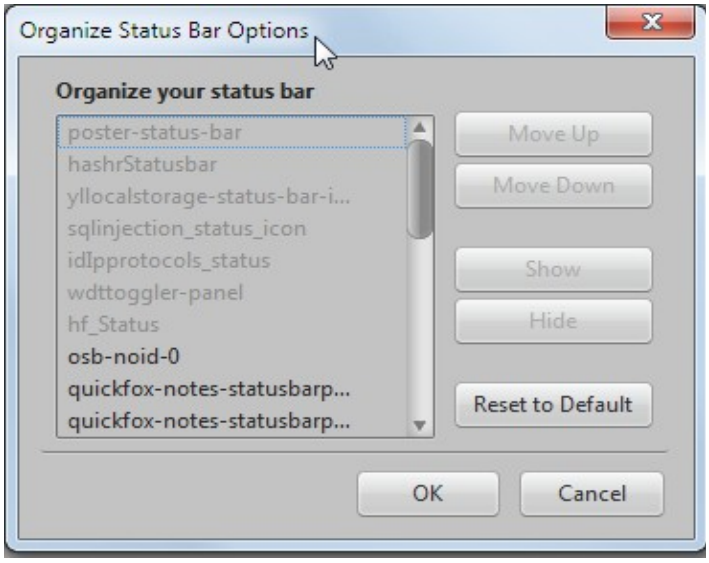


Figure 37: Status bar editor

3.5.1 Configuring Reporting

HconSTF offers different reporting options for logging web requests made using it namely,

- Centralized automatic logging – logs each and every request made in all tabs using HconSTF.
- Custom logging – separate options for which requests to log and where to log it.

Disabling centralized request logging

As it is already enabled by default and generates the log from the moment the framework is started till it is closed. It is stored on current user's desktop as,

- *http-request-log.txt* in windows
- *HconSTF_Log.txt* in linux

Disable it from:

1. Hmenu → Settings → Add-ons
2. Add-ons sidebar → HTTP Request Logger → click on disable
3. Restart HconSTF

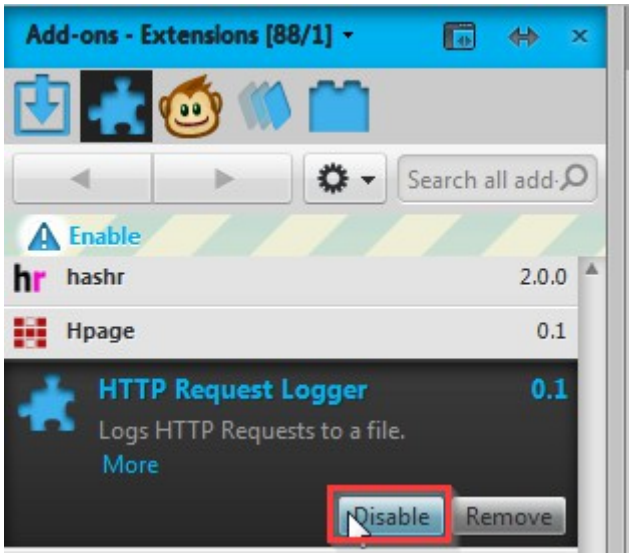


Figure 38: Disabling auto logging

Now centralized auto-logging is disabled and log on desktop will not be generated.

Setting up custom logging

Configure custom logging options from: Hmenu → Reporting → URL Logger

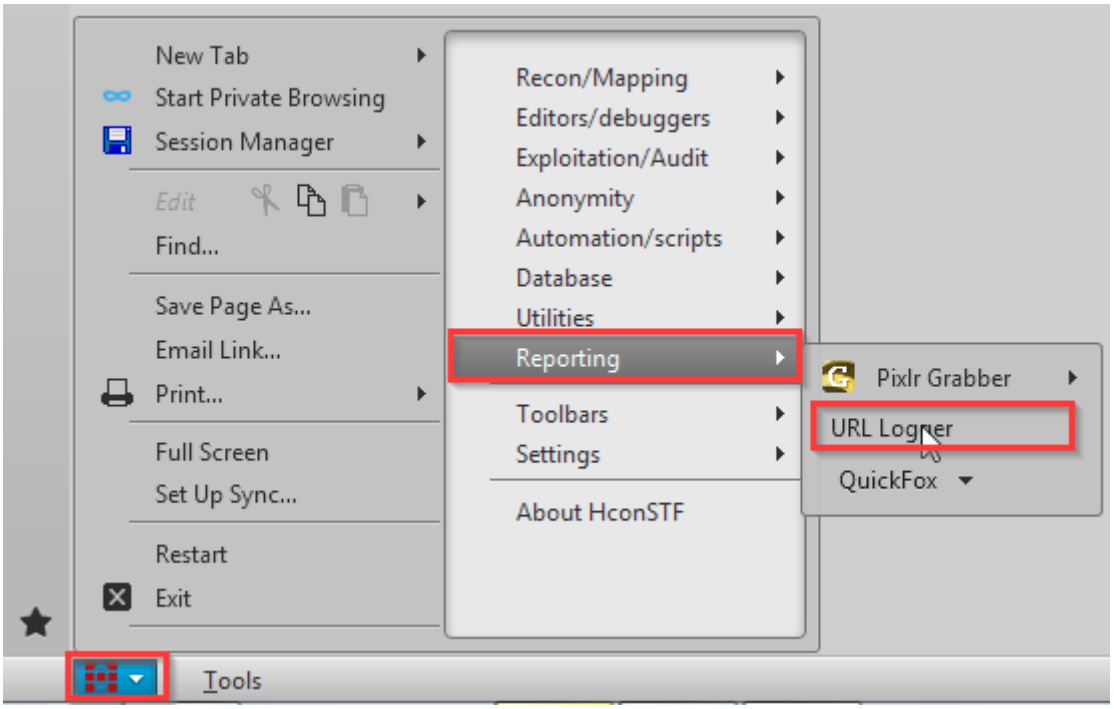


Figure 39: Url logger in Hmenu

Only check the boxes for kind of logging we needed,

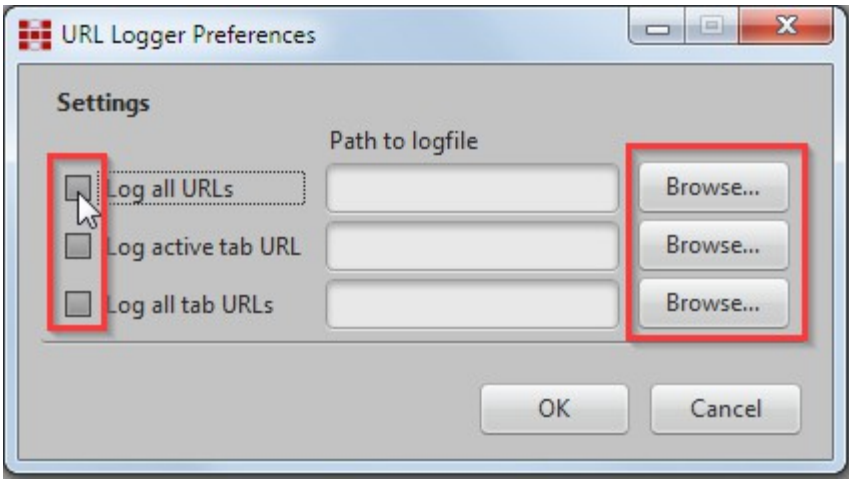


Figure 40: URL logger

Browse the directory we want to save the log at and specify a file name and save it.

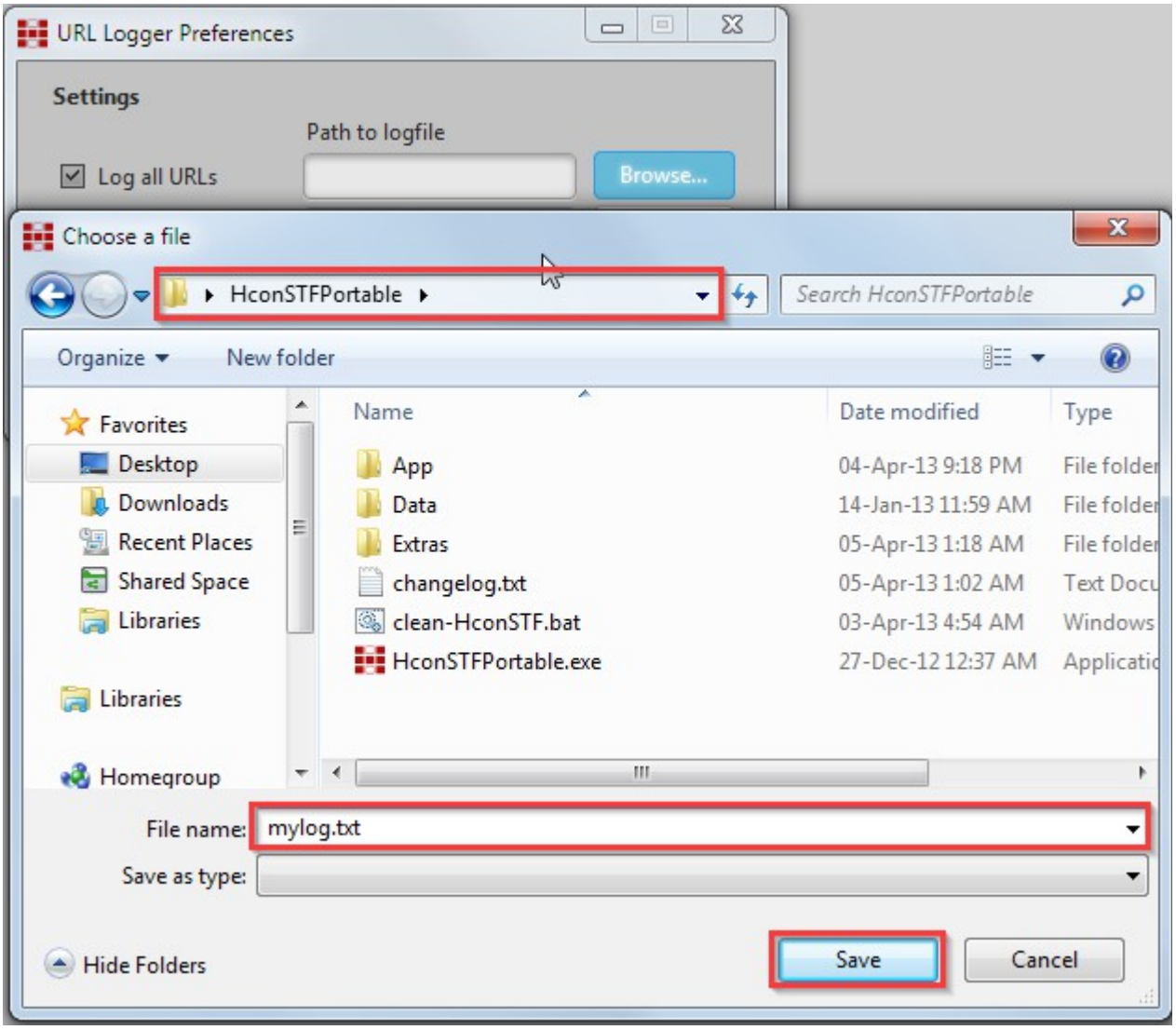


Figure 41: Location for saving log

Now it is ready and will log all requests until we uncheck the box again from the url logger preference window.

3.6 Updating HconSTF

Updating HconSTF is very simple and takes minute to do it. it updates the included inbuilt tools, scripts and search aggregator plugins but doesn't upgrade to new version of HconSTF for that check manually for the new release of it at: http://www.hcon.in/downloads.html

Update HconSTF from: Hmenu → Settings → Add-ons

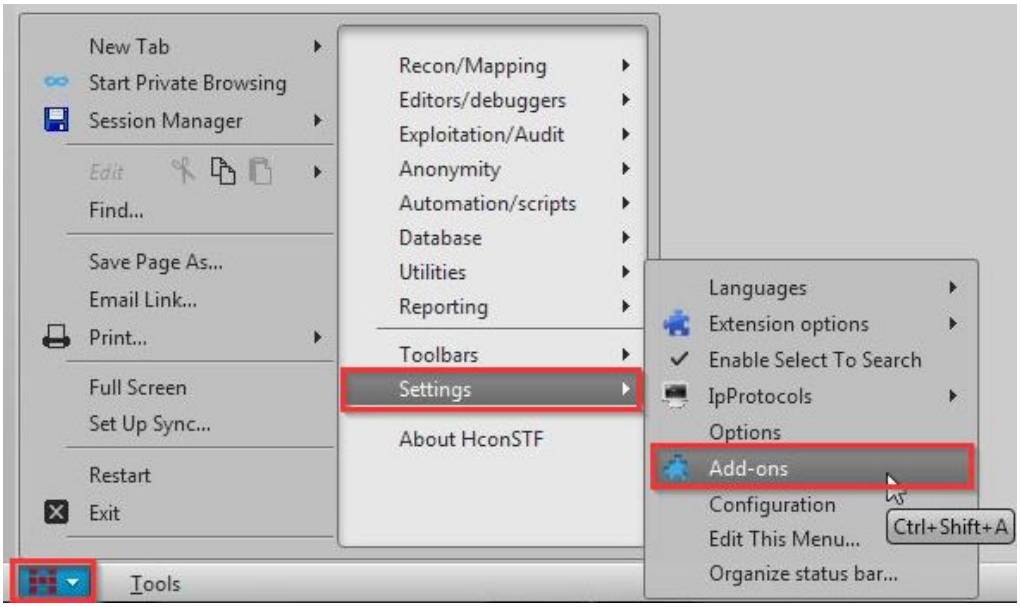


Figure 42: Opening add-ons settings

In Add-ons sidebar → Options button → Check for Updates

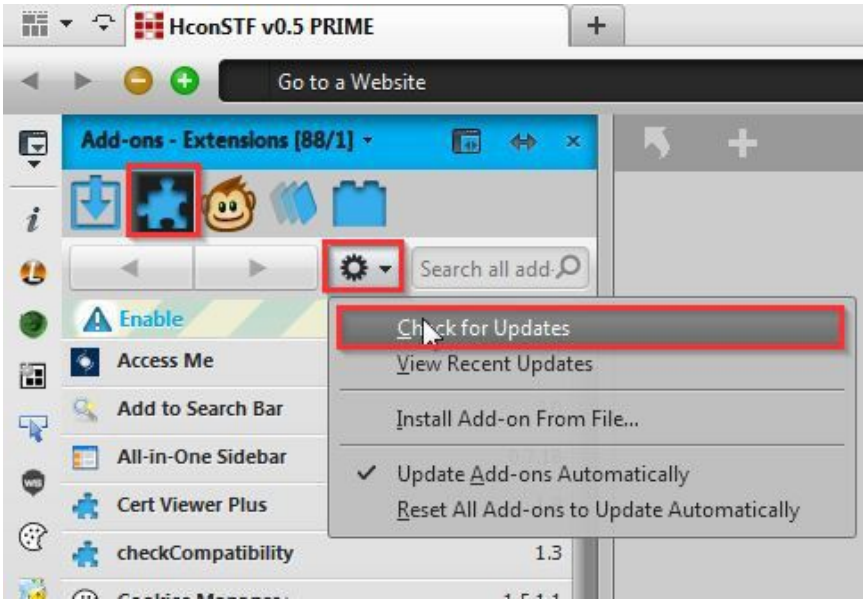


Figure 43: Checking for updates

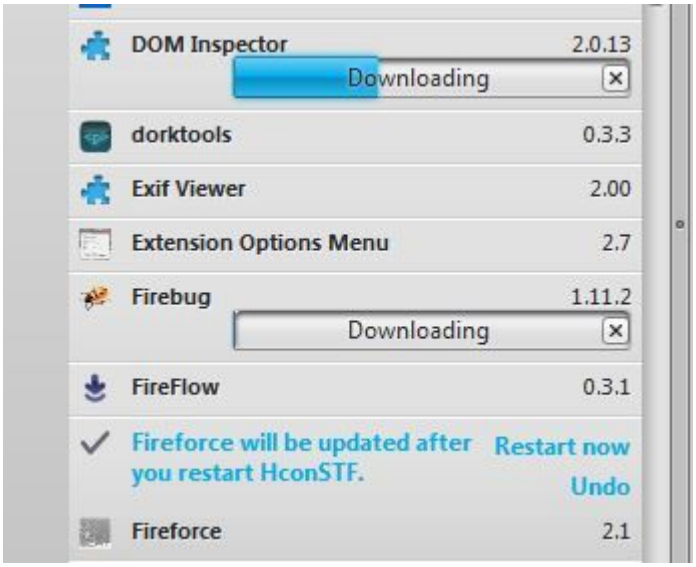


Figure 44: Updates being downloaded

After all the updates has been downloaded completely, restart HconSTF.

Note: *Make sure that to check for updates before using it, once it is updated then delete the auto generated log on the desktop as this will be containing useless entries, and restart HconSTF.*

Chapter 4: The Arsenal

In this chapter we will look at what type of toolset HconSTF provides with some unique features of HconSTF.

4.1 Categories of Tools

HconSTF can do wide verities of tasks and listed below are main functions and abilities of the framework. This is logical categorization of tools which includes tools from

Hmenu + WebUI + Search Aggregator.

1. Recon / Mapping
    - Crawling / Spidering
    - Offline browsing
    - Passive info gathering
    - Path tracing
    - Metadata analysis
    - Google Dorks
    - Doxing / Cyber spying
2. Editors / Debuggers
    - Javascript de-obfuscater
    - Web technology debuggers
    - Editors
    - Code beautifiers
3. Exploitation / Audit
    - Vulnerability scanners
        - XSS
        - DOMxss
        - SQLi
        - CMS detection
        - RFI/LFI
        - Admin Finders
        - Port scanners
    - Request manipulation
        - Manual request generation
        - Interceptor
        - Request Replay
        - Header modification

4. Anonymity
    - Darknets
        - Tor
        - I2P
        - AdvTOR
    - Proxies
        - Sock4/5
        - Web
    - Spoofing
        - User agent
        - Referrer
        - IP headers
5. Cryptography
    - Hashing
    - Encoding/Decoding
    - Identify Unknown Hash
    - Cracking Hashes
        - Bruteforcing
        - Online db checks
            - MD5
            - SHA
6. Database
    - SQLite
    - Amazon SDB
7. Scripting / Automation
    - JS attack scripts
    - Automation of tasks in framework
8. Network Utilities
    - FTP client
    - SSH client
    - CA certificate manager

9. Reporting
    - Screenshots
    - Logging
    - Note taking
    - Session saving and exporting

4.2 Special Features

HconSTF comes loaded with many special features which enhances capabilities of the whole framework and gives its users more unique way to do things.

HconSTF version 0.5 codename 'Prime' comes bundled with:

- IDB
- Search Aggregator
- Hackery Hybrid

IDB (Integrated DataBase):

IDB is Integrated database with huge number of ready to use web attack payloads for performing different attack techniques including:

- XSS
- SQLi
- LDAP
- Xpath
- XXE
- Command execution

IDB can be used in many different ways form HconSTF,

1. By activating it for injecting attack payloads in form fields

on Status bar → right click on InformEnter to activate it

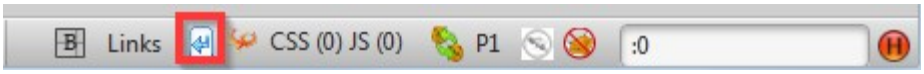


Figure 45: Activating InFormEnter

Left clicking the same will bring attack payload selection menu

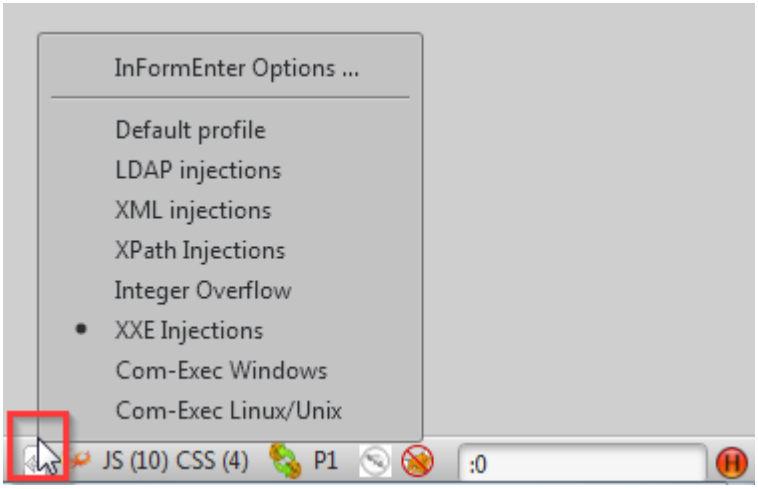


Figure 46: IDB Payloads selection menu

once it is active we can access the same selection menu from any input form filed on webpage

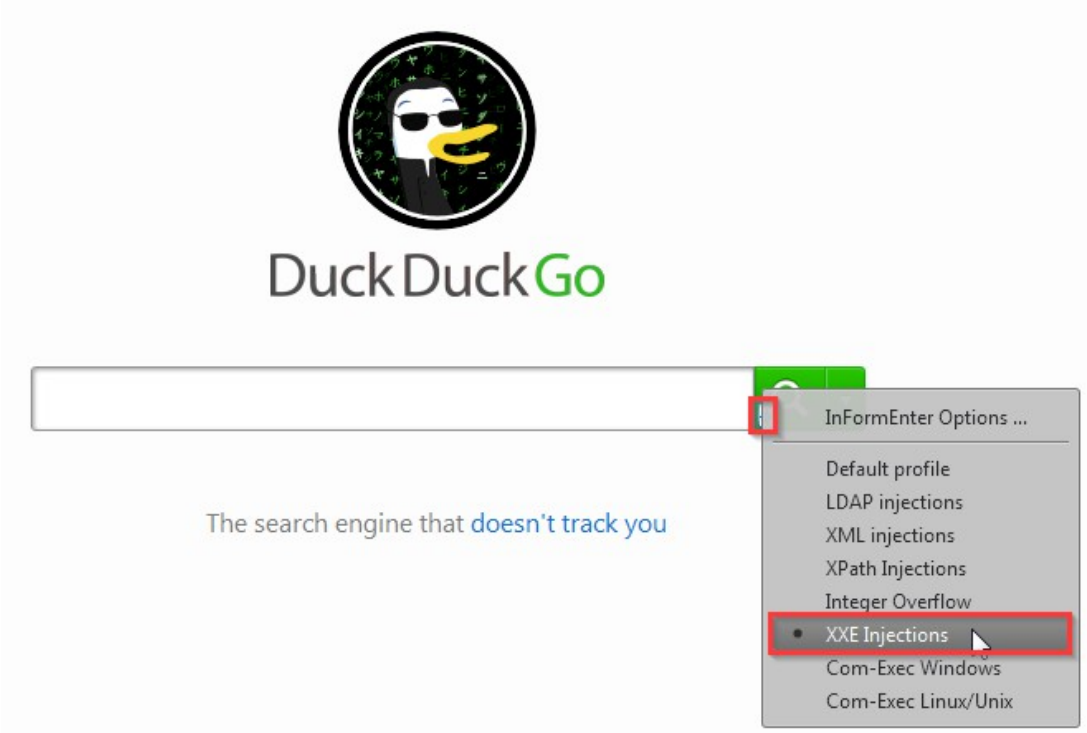


Figure 47: Selection menu on individual form fields

Left click on individual input fields will bring up all the injectable payloads also displaying number of characters in a payload.

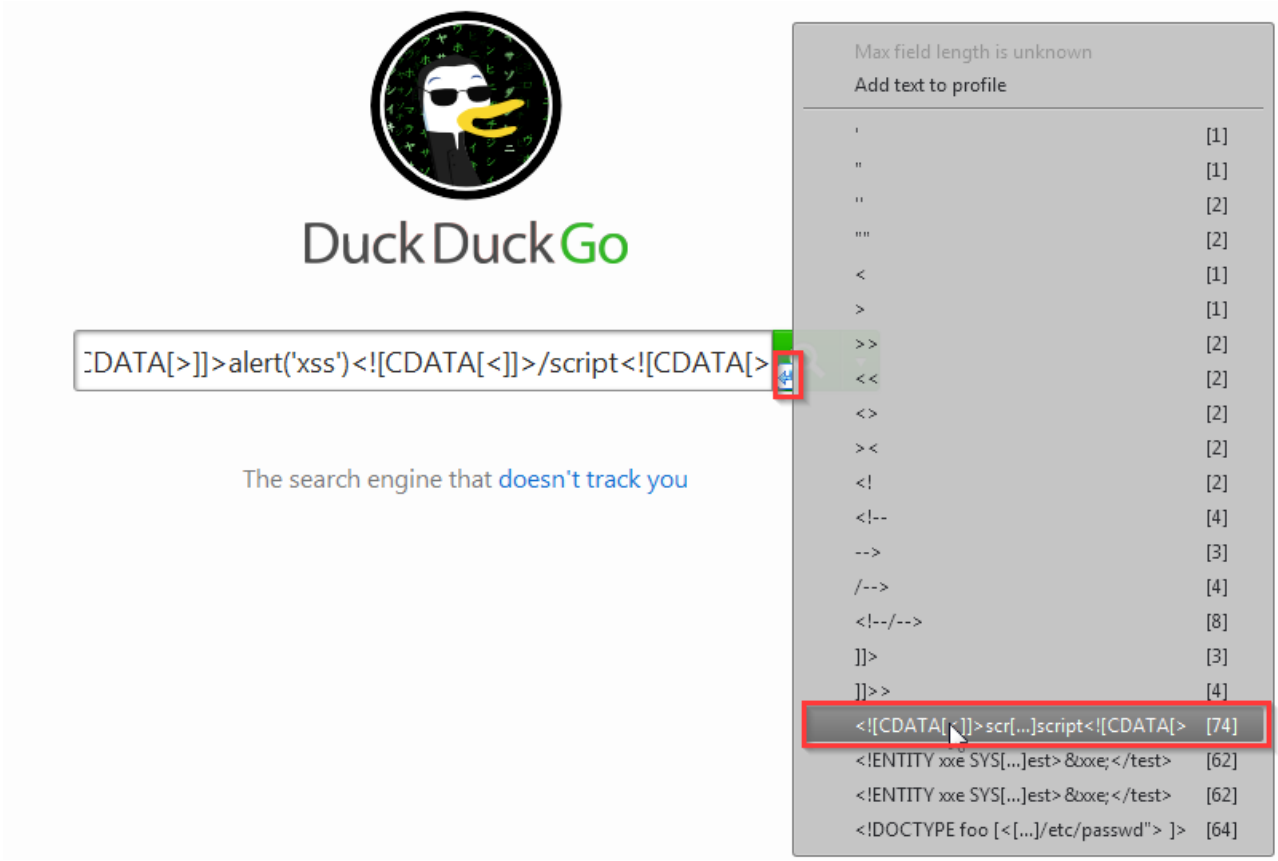


Figure 48: Injecting payloads

Note: *when it is not active it is grayed and when active it turns blue and all the input fields on web page shows inform enter icon*

2. By importing attack payloads into other tools

IDB payloads can be directly imported into tools such as

- Sql Inject me
- XSS me
- Search XSS scanner

Import files can be found in 'Extras/IDB' directory under HconSTF main directory, use the configuration menu of individual tool mentioned to import this files.

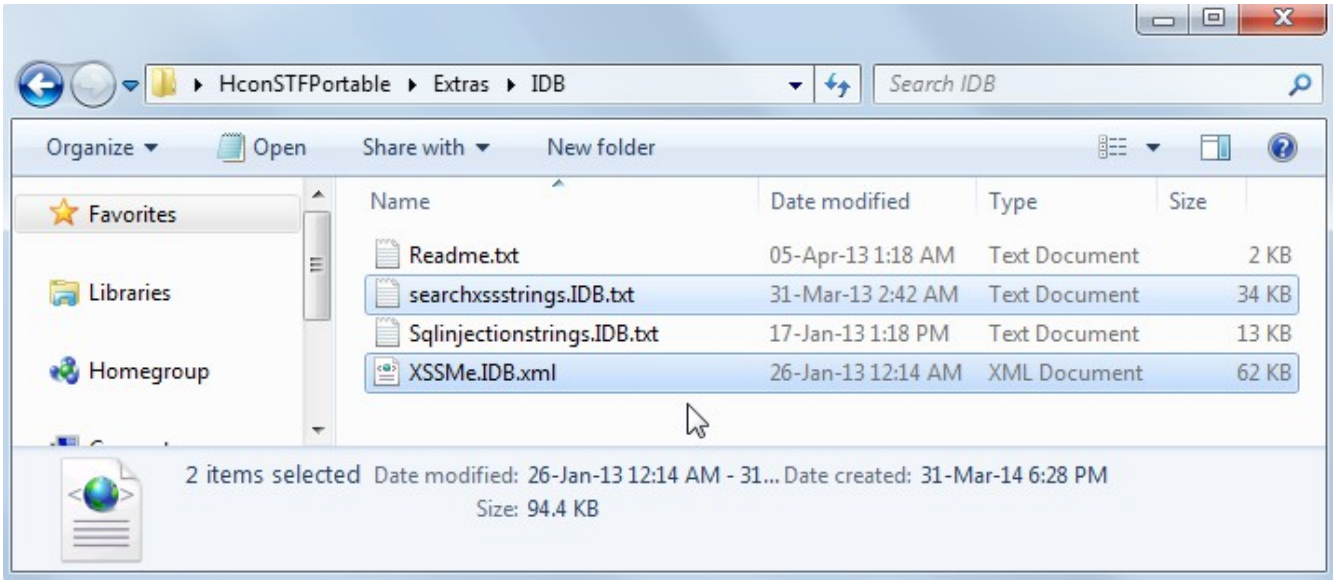


Figure 49: Ready to import files in Extras directory

Search Aggregator:

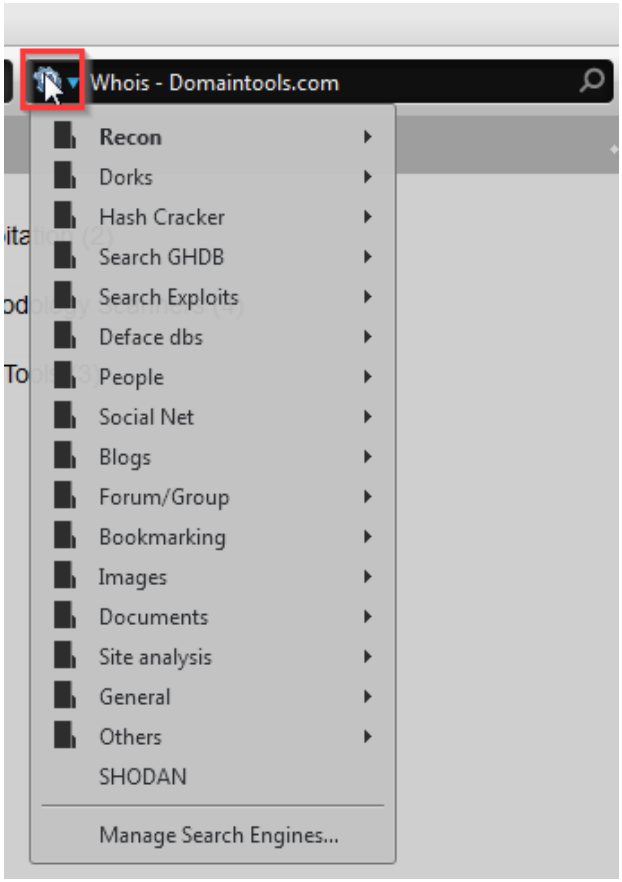


Figure 50: Search Aggregator

Tool for searching the web and getting the meaningful data as quick as possible, Helps in many open source intelligence based tasks like,

- Passive Web & Network Reconnaissance
- Doxing
- Cyber Spying
- Hash cracking

more than 165+ Plugins in current version.

Under each category there are several plugins we can run all in a single click or can just paste the search term and select the search plugin one by one from any category and it will open up each result in a new tab.

Hackery Hybrid:

Its a collection of huge amount of learning bookmarks for any techniques, tools, reference material, courses, tutorial videos and much more in categories.

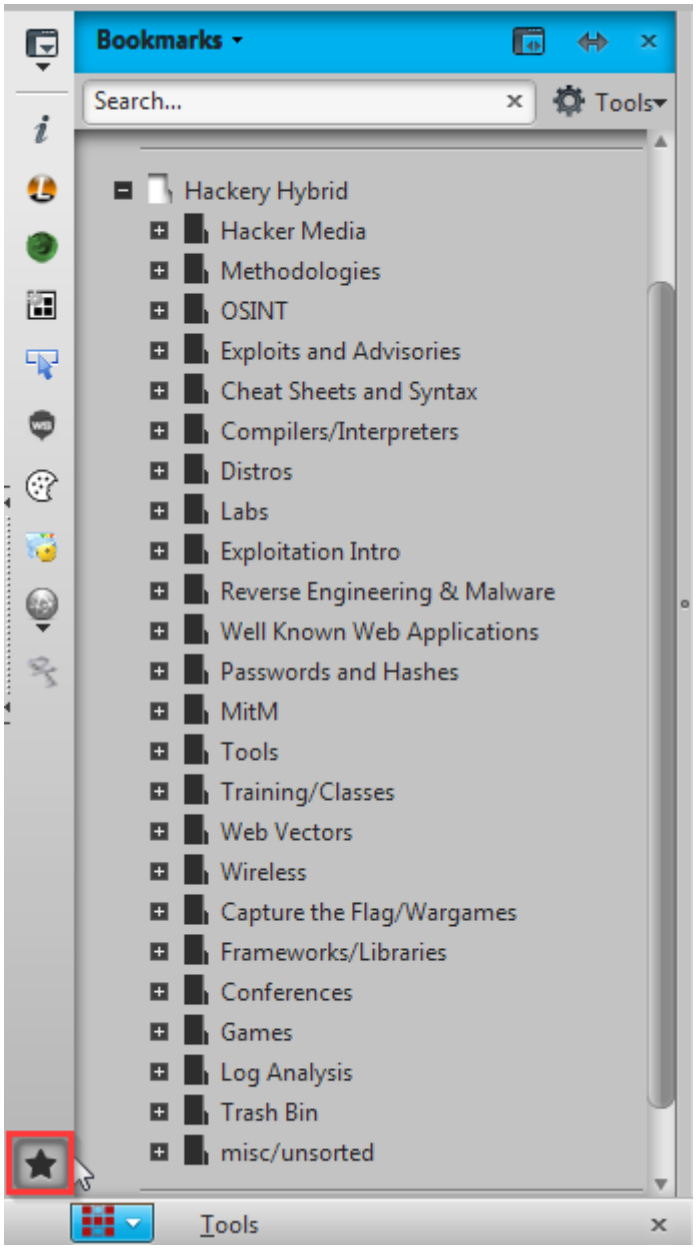


Figure 51: Hackery Hybrid

4.3 Miscellaneous: Extras Directory & HconSTF-Cleaner

Other then the features and toolset we discussed in previous sections there are few more noticeable components of HconSTF like,

'Extras' Directory:

This directory is located in main directory of the HconSTF. This directory includes help and other related files for tools in HconSTF and includes the IDB (Integrated Database) with ready to import payload strings.

HconSTF-Cleaner:

Its a simple shell script which helps HconSTF in running smoothly, removes unwanted and temporary files generated during each session and resets the whole HconSTF session for a fresh start.

- For windows:

  It is located as a separate file HconSTF-cleaner.bat just double click on it to run it.

- For Linux:

It is a part of the main Launcher, so when we close the HconSTF gui window, in our console launcher it will ask us "Run HconSTF cleaner now?" and according to our choice then it exits.

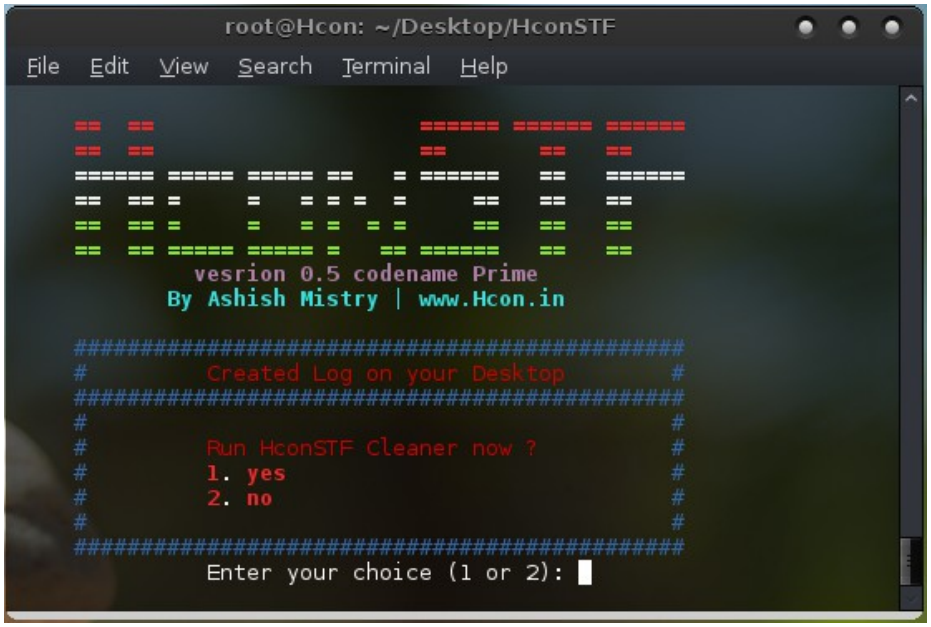

root@Hcon: ~/Desktop/HconSTF
File Edit View Search Terminal Help
vesrion 0.5 codename Prime
By Ashish Mistry | www.Hcon.in
Created Log on your Desktop
Run HconSTF Cleaner now ?
1. yes
2. no
Enter your choice (1 or 2):

Figure 52: HconSTF Cleaner under linux

Note: *For editing the cleaner and customize it just open it with a text editor, HconSTF-cleaner.bat in windows and HconSTF main launcher in linux.*

Warning: *When done with web application penetration testing on our target then do take all the text, screenshots and logs to a separate directory and run HconSTF cleaner, until and unless done with current web application don't run the cleaner, as it will delete all the data generated.*

4.4 Tools Listing

4.4.1 Add-ons

Number of Add-ons: 89

Access Me 0.2.4	InFormEnter 0.6.3
Add to Search Bar 2.0	ipFuck 1.0.1
All-in-One Sidebar 0.7.18	IpProtocols 0.2.1
Cert Viewer Plus 1.9	IPvFox 0.8.3
checkCompatibility 1.3	Link Gopher 1.3.2
Cookies Manager+ 1.5.1.1	Live HTTP headers 0.17
CookieSwap 0.5.284	Locale Switcher 3
CryptoFox 2.2	Menu Editor 1.2.7
DOM Inspector 2.0.14	Meta Generator Version Check 1.0.24
dorktools 0.3.3	MM3-ProxySwitch 2013.92
Exif Viewer 2.00	Modify Headers 0.7.1.1
Extension Options Menu 2.7	NoScript 2.6.6 (Disabled)
Firebug 1.11.2	Organize Search Engines 1.7
FireFlow 0.3.1	Organize Status Bar 0.6.4 (Incompatible)
Fireforce 2.1	Personal Menu 5.1.0
FireFTP 2.0.7	Phoenix 1.7.5
FirePath 0.9.7	Pixlr Grabber 2.1.1
FirePHP 0.7.2	Poster 3.1.0
Fireshark 1.1	Proxy Tool 1.17
FireSSH 0.92.2	QuickFox Notes 2.8.0
FireStorage 1.0.2	Ra.2: DOM XSS Scanner 0.3 beta
Flagfox 4.2.8	RefControl 0.8.16
FlashFirebug 4.67	RESTClient 2.0.3
FormFox 1.7	Resurrect Pages 2.0.6
FoxyProxy Standard 4.1.3	SDBizo 2011.07.22.0000
Greasemonkey 1.8	Search on Engine Change 1.2
Groundspeed 1.2	SearchXSS 1.0.1
HackBar 1.6.2	Secure Or Not 1.2

hashr 1.2	Select To Search 2.0
Hpage 0.1	Selenium Expert (Selenium IDE) 0.25
HTTP Request Logger 0.1	Selenium IDE 1.10.0
HttpFox 0.8.11	Selenium IDE: C# Formatters 1.10.0
HttpRequester 1.0.4	Selenium IDE: Java Formatters 1.10.0
iMacros for Firefox 8.3.0	Selenium IDE: Python Formatters 1.10.0
Selenium IDE: Ruby Formatters 1.10.0	UI Fixer 1.4.4
Session Manager 0.8.0.1	URL Flipper 3.1.1.20
Session Manager Export Tool 0.2	URL Logger 1.0.3
Spider 0.0.5.0	User Agent Switcher 0.7.3
SpiderZilla 1.6.0	View Dependencies 0.3.3.2
SQL Inject Me 0.4.6	Wappalyzer 2.7.0
SQL Injection! 1.3 (Incompatible)	Web Developer 1.2.2
SQLite Manager 0.7.7	Websecurify 2.0.5
Tamper Data 11.0.1	XPather 1.4.5 (Incompatible)
Tile Tabs 9.1	XSS Me 0.4.6
Toggle Web Developer Toolbar 4.2	

4.4.2 Search Aggregator Plugins

Number of Search Plugins: 169

123peoplecom	google-blog-search
1337day-inj3ct0r-exploit-db	google-dorks--advisories--vulnerabilities
add-attackcom	google-dorks--error-messages
admin-finder	google-dorks--files-containing-juicy-info
aljyyoshorg	google-dorks--files-containing-passwords
amazondotcom	google-dorks--files-containing-usernames
anqelpl	google-dorks--footholds-
archives-files-search	google-dorks--network-or-vulnerability-data
as-report	google-dorks--pages-containing-login-portals
askcheckcom-sha1	google-dorks--sensitive-directories
askcheckcom	google-dorks--sensitive-online-shopping-info
authsecucom	google-dorks--various-online-devices
backup-files-search	google-dorks--vulnerable-files
bigtrapezecom	google-dorks--vulnerable-servers
bing-ip-to-host	google-dorks--web-server-detection
bing	google-groups
blogcatalogcom-blogs	google
blogcatalogcom-connect	hack-dbcom
blogcatalogcom-users	hack-mirrorcom-in-archive
blogcatalogcom	hack-mirrorcom-in-onhold
boardreader	hack-mirrorcom-in-spcl-archive

boardtrackercom	hash-killercom
builtwith-technology-lookup	hashcheckerde---45hash-crackers
buzzfeed	host-spy
cloudcrackernet-sha1	icerocketcom
cloudcrackernet	icmp-traceroute
config-files-search	infosniper
cve-dictionary-search-suggest	instagram-search
decrypt-md5com	internal-link-search
decrypterco-sha1	ip-adresscom
decrypterco	ip-information
default-passwords--cirtnet	ip2locationcom
default-ports--cirtnet	iscsansedu-sha1
deliciouscom	iscsansedu
document-files-search	kinginfetnet
domain-dossier	knowem-socialnet
domaintoolscom	knowem2
duckduckgo	linkedin
eBay	livejournal-blogs
edocrcom	md5-dbde
email-search	md5-decryptercom
facebook	md5-lookupcom
firefox-add-ons	md51altervistaorg
flickr	md5crackcom
friendfeed	md5crackerwebnet32com
md5hoodcom	md5gromwebcom
md5my-addrcom	md5hashcrackingcom
md5myinfosecnet	sitemap-blogger
md5net	sitemapxml
md5noisettech	slashdotorg
md5onlinenet-1	slideboomcom
md5passcom-sha1	slideshare-search
md5passcom	social-mention
md5passinfo	stringfunctioncom-sha1
md5rainbowcom	stringfunctioncom
md5rcom	sub-domain-search
md5rednoizecom-sha1	tcp-traceroute
md5rednoizecom	technoraticom-blogs
mirror-macom	technoraticom-post
misc-search	the-mail-archive
mmkeycommd5	tobtucom
netcraft---uptime	toolsbenramseycom
netcraft-toolbar	twitpiccom
netmd5crackcomcracker	twitter
ns-report	udp-traceroute
offensive-security-exploit-database	urlvoidcom
omgili	userpass-search
online-domain-toolscom-	w3tech-site-info

online-domain-toolscom	webmii
onlinehashcrackcom-sha1	whois-by-ip-address
onlinehashcrackcom	whostalkincom
openbook	wikipedia
osvdb	wwwmd5-hashcom
oval-repository-search-suggest	xssed-search
packetstorm-search-suggest	yahoo
pcapr-search-	zone-hccom
pdf-search	zone-horg
peekyou--user-name	scribdcom
people-search-engine	search-100-engines
picfogcom	securityfocus-vulns-search-
pinterestcom	securitywire-search
redditcom	sha1-lookupcom-sha1
requnixtk	shodan-exploits
rfc-keywords-search-	shodan
robotstxt	

4.4.3 GreaseMonkey Scripts

Number of scripts: 18

ClickJacky	PostIntercepter
Flickramio	Sitemaps_Generator_for_Blogger
GCHiddenText	WebAcid
Hackthissite_Hacking_Tool	WebPageFingerPrint_v0.4
Hackvertor	XSS-1
IPCountryLookup	xssearcher
Malware_Script_Detector_v.02b	XSS_Detective
Malware_Script_Detector_v_1.1	XSS_Detective_Test_Vectors
phpsecinfo_checkerv.01	XSS_This_Page

Chapter 5: Web Application Penetration Testing with HconSTF

In this chapter we will look at how to perform some basic web app pentesting related tasks using HconSTF.

5.1 Information Gathering & Initial Analysis

As a start in any security audit methodology we will going to take information gathering as first step using HconSTF.

- Mapping: We initially try to understand the structure of the web application.
- Reconnaissance: We understand what technologies are in place in the web application for its running, including webserver, web frameworks, libraries etc.

5.1.1 Mapping

We will going to look at some of the features of HconSTF to map and understand the web infrastructure of our target using passive techniques.

Crawling / spidering - to understand the pages and directory structure

- Links extraction from page: Right click on 'LINKS' on status bar → 'Extract all links'

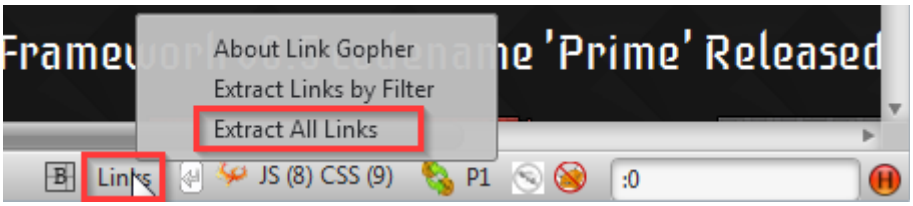


Figure 53: Extracting all links from webpage

It will list all the links and connected domains in a single webpage which can be saved as html

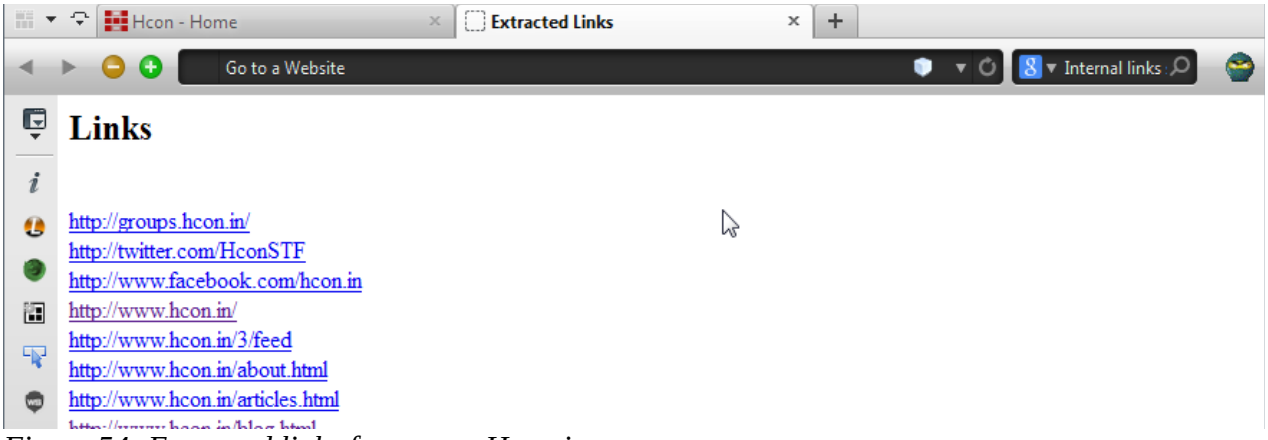


Figure 54: Extracted links from www.Hcon.in

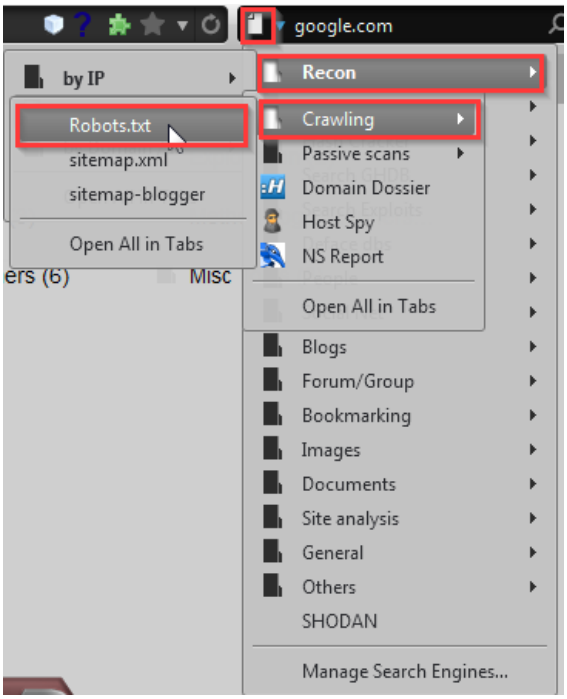


Figure 55: Crawling with search aggregator

- Robots.txt - Another quickest way to map the target

Type target link in search aggregator,

Goto Recon → by Domain → Crawling → Robots.txt

As robots.txt is the easiest way to see which path, web admin doesn't want to be seen by anyone.

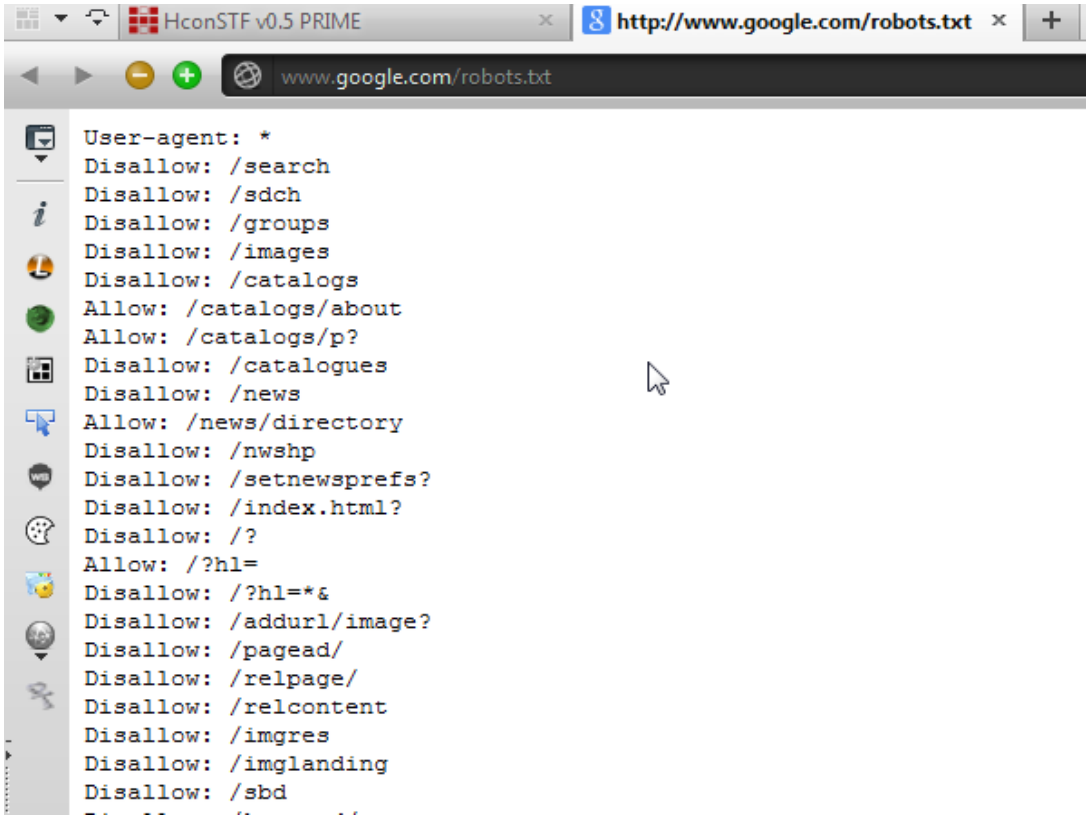


Figure 56: Robots.txt of google.com

Google Dorks

Gathering information on email, sub domains, files for meta data analysis etc.

There are many dorks for mapping the infrastructure of target,

- For searching file types
- For searching emails
- For searching sub domains and many more

Access all this from: search aggregator → dorks

we will going to run all the dorks at once on Hcon.in

This will going to run all the dorks and will show information in a new tab for each dork, so that we can manually inspect results.

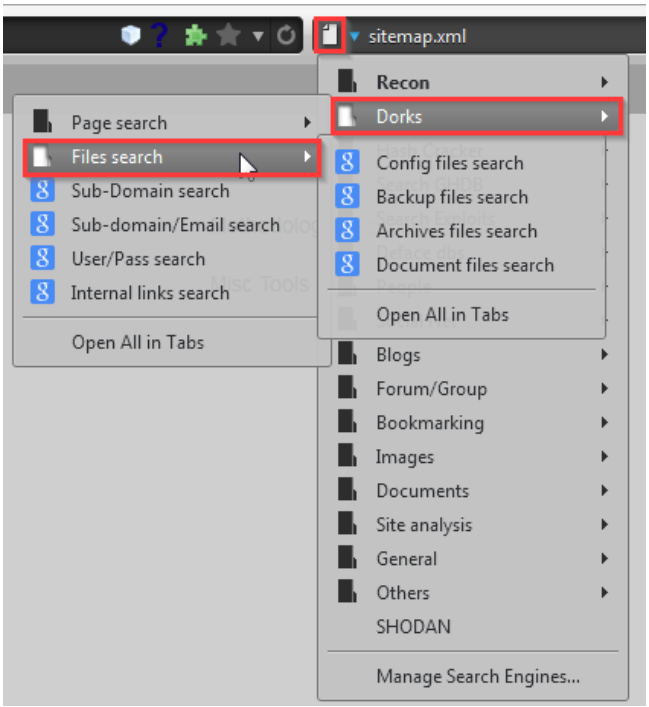


Figure 58: All dorks in search aggregator

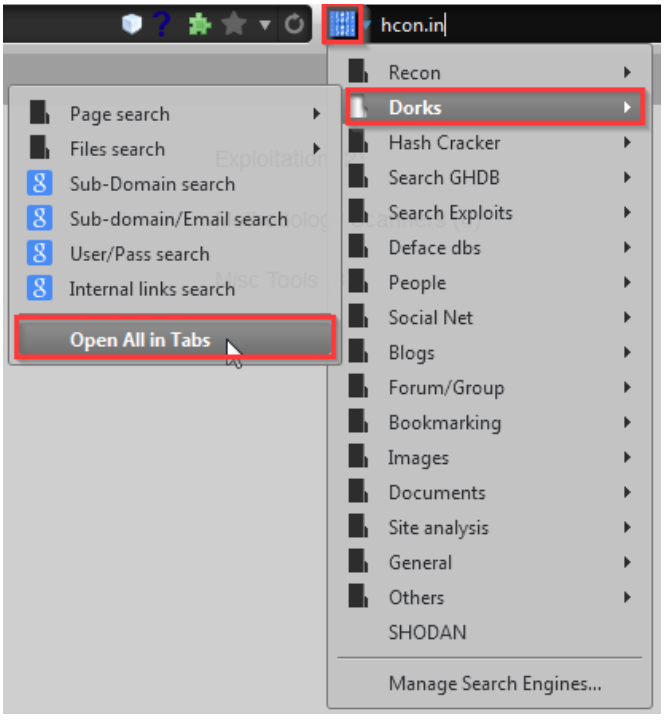


Figure 57: Run all dorks on www.Hcon.in

Shared hosting test

Check if the target is hosted on a shared web hosting or not, for using this we need public IP address of the target, paste it in search aggregator, goto Recon → by IP → bing IP to host

this will going to show other websites which are hosted on the same IP address. for this demo we are using IP address of site www.Hcon.in

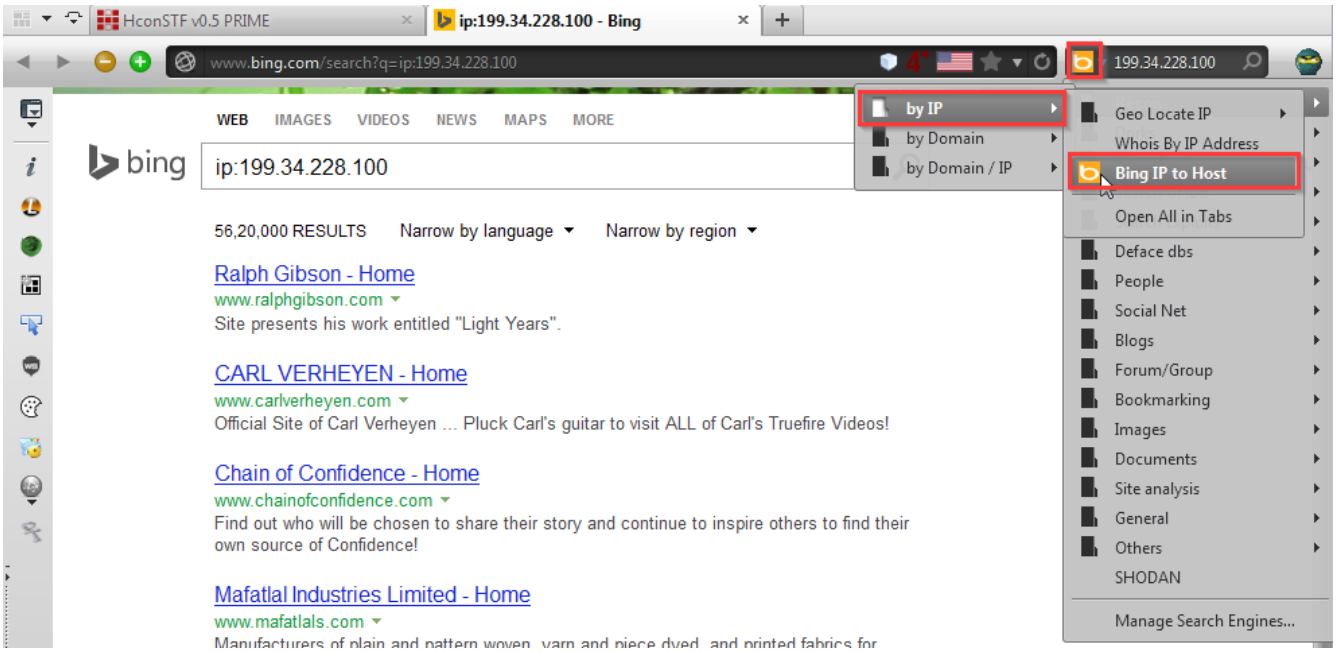


Figure 59: Other sites hosted on same IP address of Hcon.in

5.1.2 Reconnaissance

HconSTF is feature rich for doing passive reconnaissance using offline and online tools. We will be using HconSTF to perform several tasks like,

- Technologies used in website
- Get Full domain report
- Server information
- Checking for open ports and services
- CMS and version detection

Technologies used in website

We will going to use search aggregator → Recon → by Domain → Passive scans → Builtwith Technology Lookup

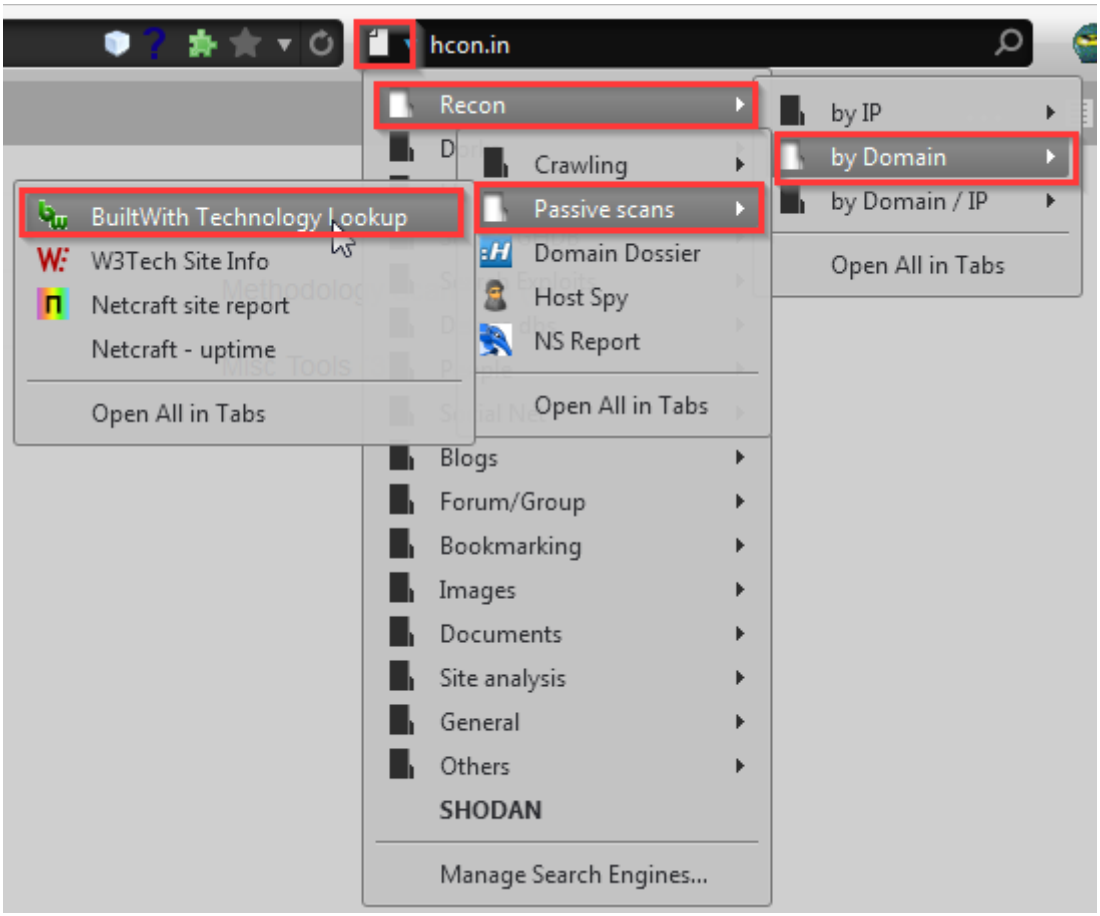


Figure 60: Passive lookup for technologies used in a website

As we can see all of the technologies used in that domain are listed including information like domain registrar, web server, web libraries with version, CMS, hosting provider.

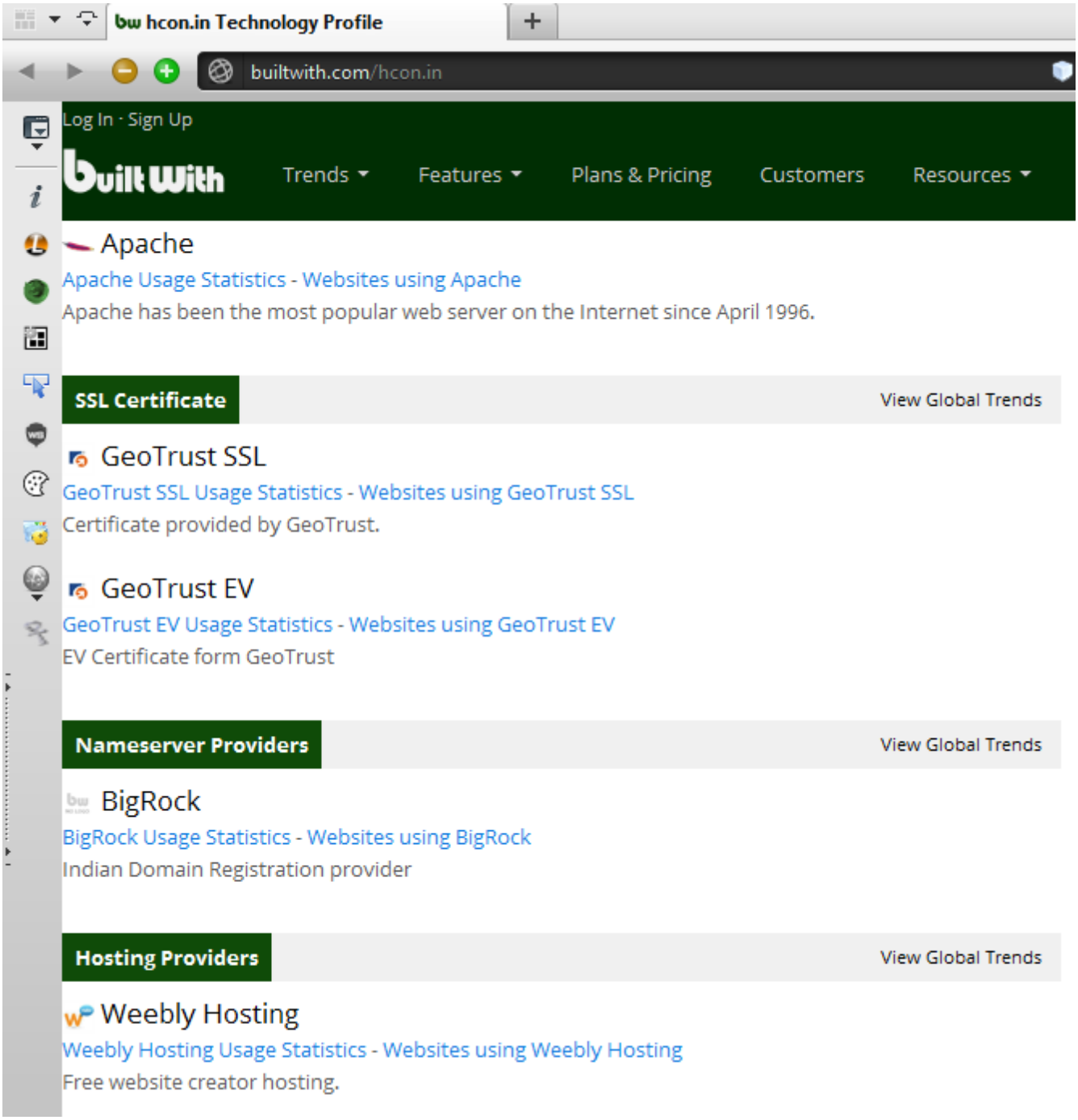


Figure 61: Results of scan showing technologies used in Hcon.in

This is totally passive and done in moments.

Full domain report

Using search aggregator → Recon → by Domain → Domain Dossier, we can give IP address or domain name as input for this.

The generated report consists of,

- domain whois records
- network whois records
- DNS records
- traceroute
- port & service scan information

and its all passive as we are not sending any direct network packets to the target host.

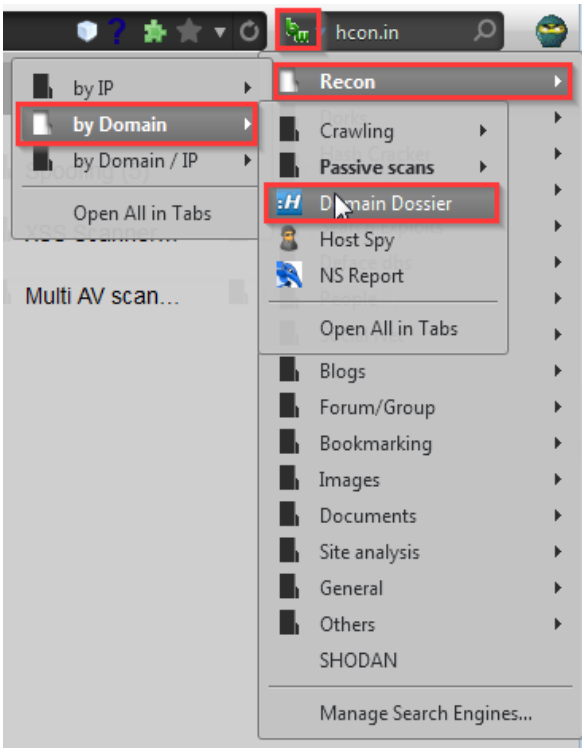
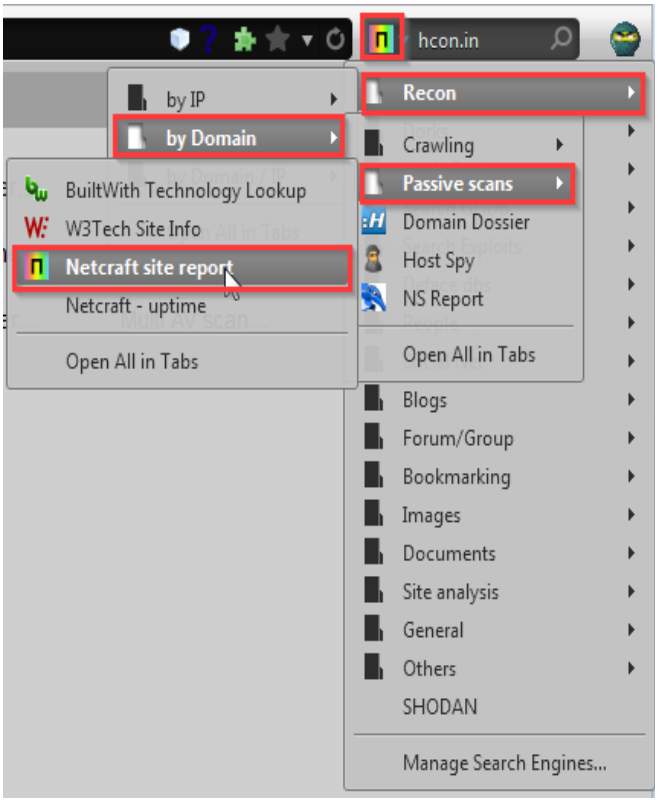


Figure 62: Domain dossier for domain report

Figure 63: Domain dossier results

Server related info

We can find when the server was last updated, which Operating system it is running, where it is located etc. for that we will going to use search aggregator → recon → by Domain → Passive scans → Netcraft site report.



This makes easy for us to understand technology profile of the target, report shows security index, OS and web server information and more.

Figure 64: Server information using netcraft

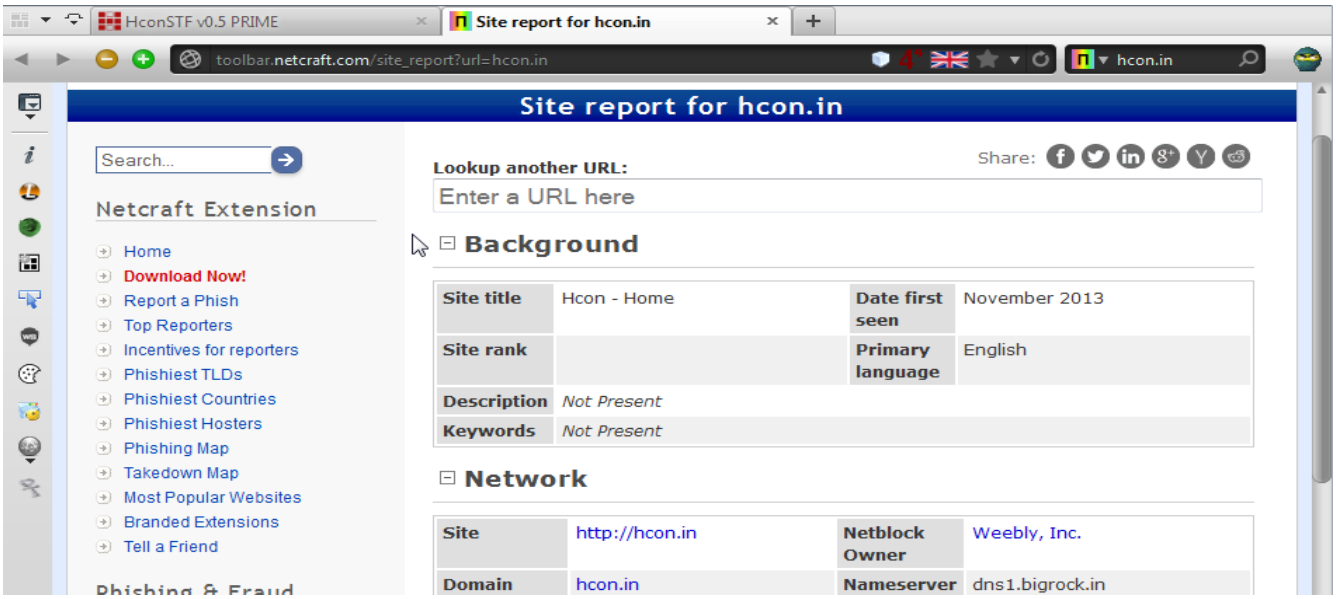


Figure 65: Hcon.in server information

We can see the same with offline tools

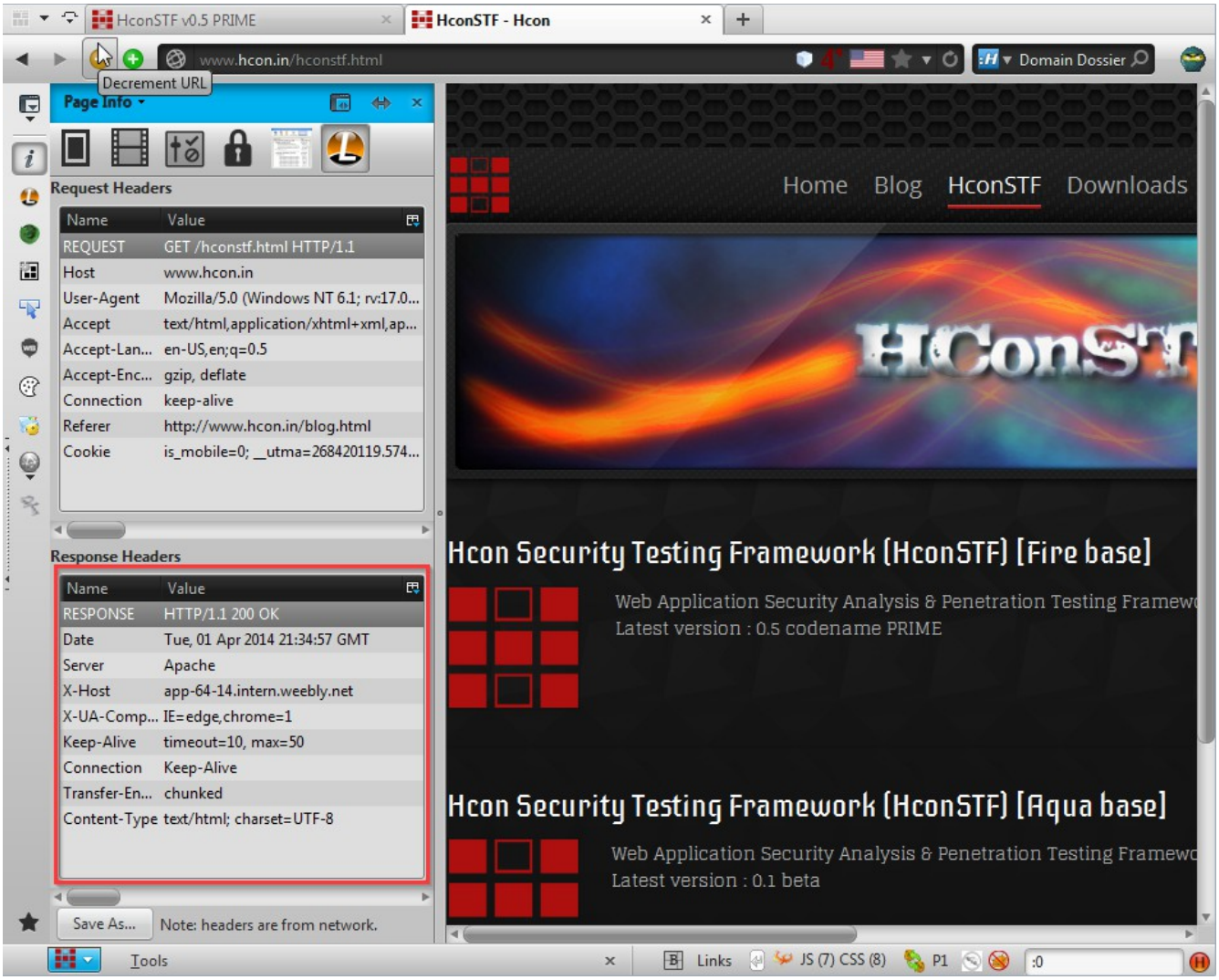


Figure 66: Response headers containing information

As we can see in request and response headers we can find lot of information like server, OS, Host etc. This information varies if the site is properly secured else we can even see the web server and OS versions in headers.

Checking for open ports and services

We got the ports and services information in full domain report section but let us try to use more specific tools for port scanning. We will going to use tools from WebUI of HconSTF which uses external web services, as there are many port scanners available.

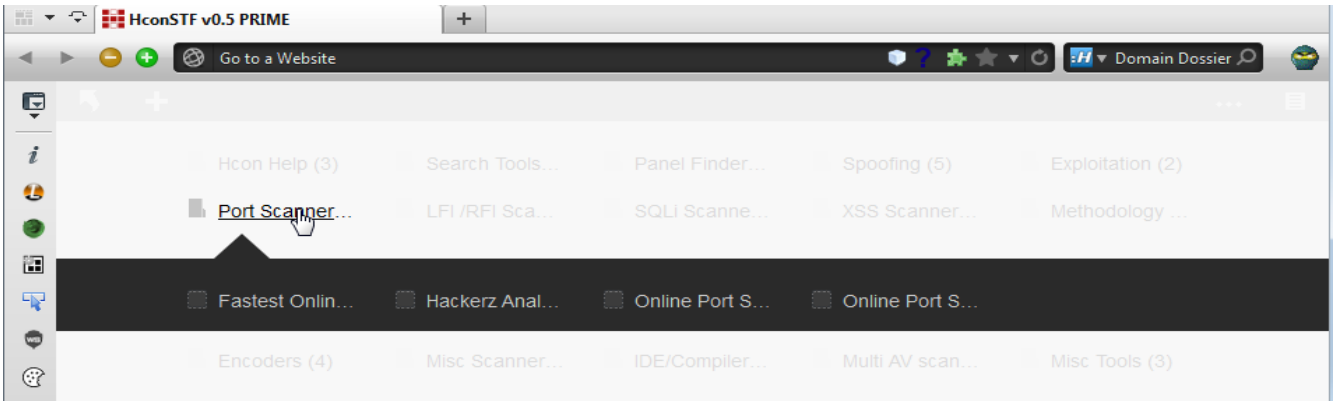


Figure 67: Running port scanners from WebUI

We selected one from the port scanners available. We can give IP address or Host as target and can scan for a specific port rage or specific set of ports or some more popular ones.

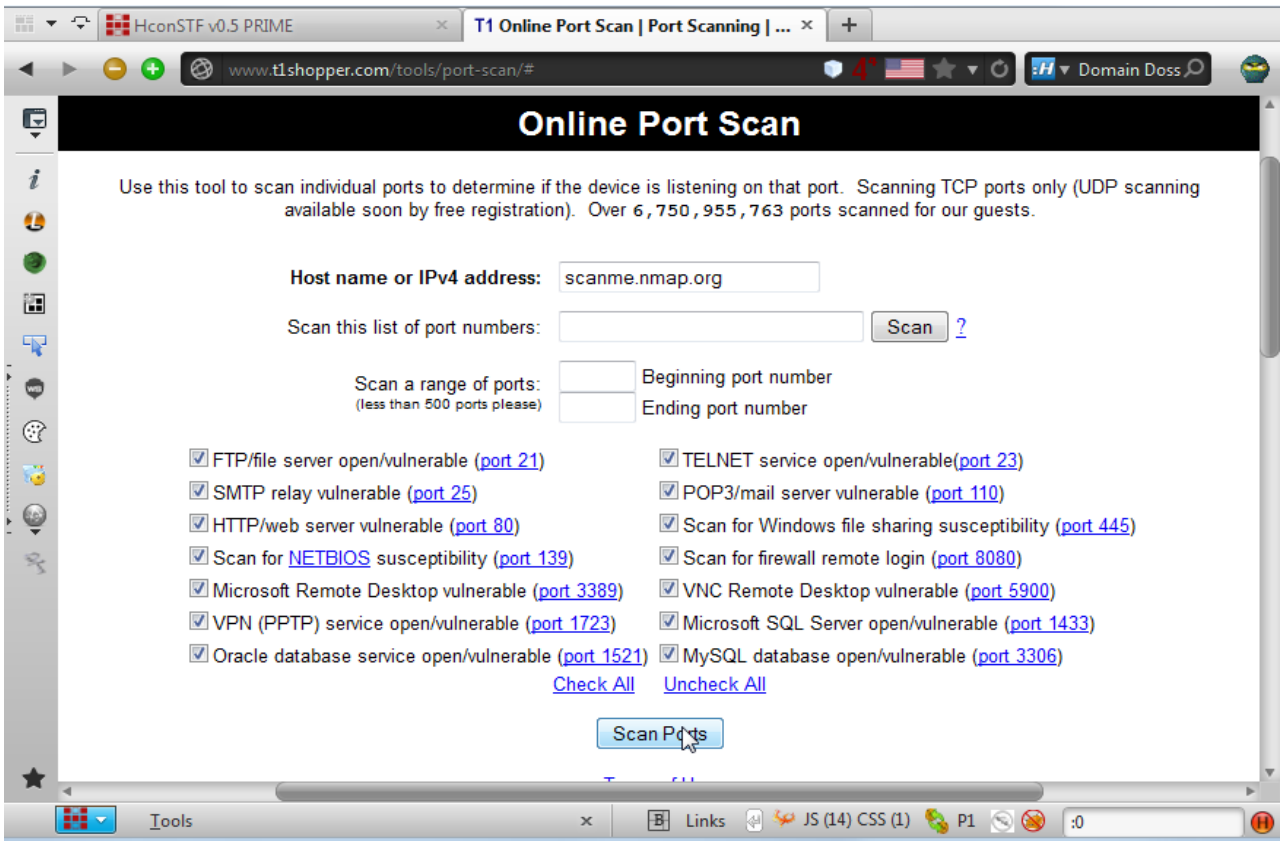

HconSTF v0.5 PRIME
T1 Online Port Scan | Port Scanning | ...
www.t1shopper.com/tools/port-scan/#
Domain Doss
Online Port Scan
Use this tool to scan individual ports to determine if the device is listening on that port. Scanning TCP ports only (UDP scanning available soon by free registration). Over 6,750,955,763 ports scanned for our guests.
Host name or IPv4 address:
scanme.nmap.org
Scan this list of port numbers:
Scan
?
Scan a range of ports:
(less than 500 ports please)
Beginning port number
Ending port number
FTP/file server open/vulnerable (port 21)
SMTP relay vulnerable (port 25)
HTTP/web server vulnerable (port 80)
Scan for NETBIOS susceptibility (port 139)
Microsoft Remote Desktop vulnerable (port 3389)
VPN (PPTP) service open/vulnerable (port 1723)
Oracle database service open/vulnerable (port 1521)
TELNET service open/vulnerable(port 23)
POP3/mail server vulnerable (port 110)
Scan for Windows file sharing susceptibility (port 445)
Scan for firewall remote login (port 8080)
VNC Remote Desktop vulnerable (port 5900)
Microsoft SQL Server open/vulnerable (port 1433)
MySQL database open/vulnerable (port 3306)
Check All
Uncheck All
Scan Ports
Tools
Links
JS (14) CSS (1)
P1

Figure 68: Configuring Nmap scan

We scanned for 21,22,25,80,443,8080 on scanme.nmap.org and we found some good results, we can scan for entire port number range but that will be more time consuming.

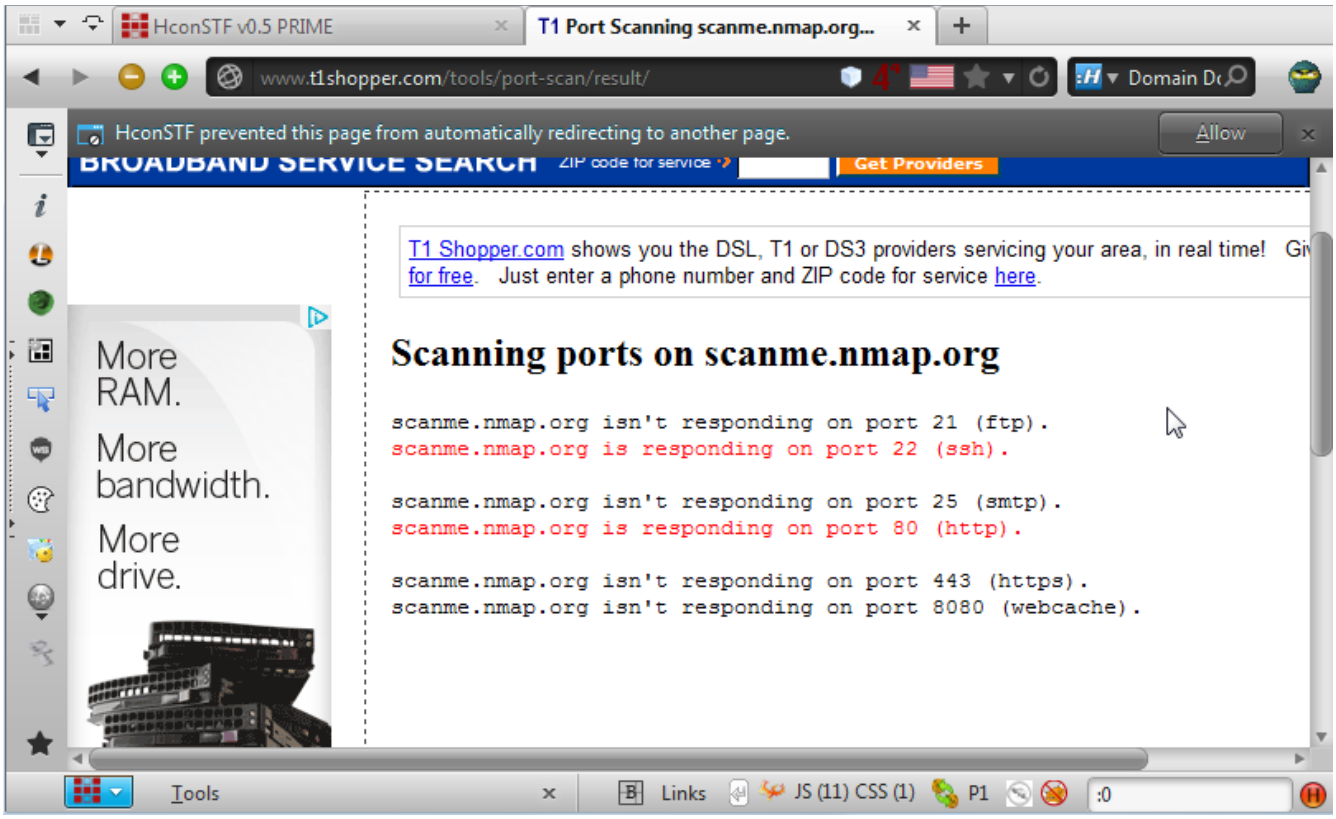

HconSTF v0.5 PRIME
T1 Port Scanning scanme.nmap.org...
www.t1shopper.com/tools/port-scan/result/
HconSTF prevented this page from automatically redirecting to another page.
Allow
Get Providers
T1 Shopper.com shows you the DSL, T1 or DS3 providers servicing your area, in real time!
for free. Just enter a phone number and ZIP code for service here.
Scanning ports on scanme.nmap.org
scanme.nmap.org isn't responding on port 21 (ftp).
scanme.nmap.org is responding on port 22 (ssh).
scanme.nmap.org isn't responding on port 25 (smtp).
scanme.nmap.org is responding on port 80 (http).
scanme.nmap.org isn't responding on port 443 (https).
scanme.nmap.org isn't responding on port 8080 (webcache).
More RAM.
More bandwidth.
More drive.
Tools
Links
JS (11) CSS (1)
P1

Figure 69: Results of online Nmap scan

Note: *We can also use nmap directly from HconSTF or specific IP address just by selecting it that is covered in chapter 8.1*

CMS and its version detection

When we open the site in HconSTF and if the target site uses any known CMS then HconSTF will flag it directly.

mediawiki v1.16.2 is running on STK site:

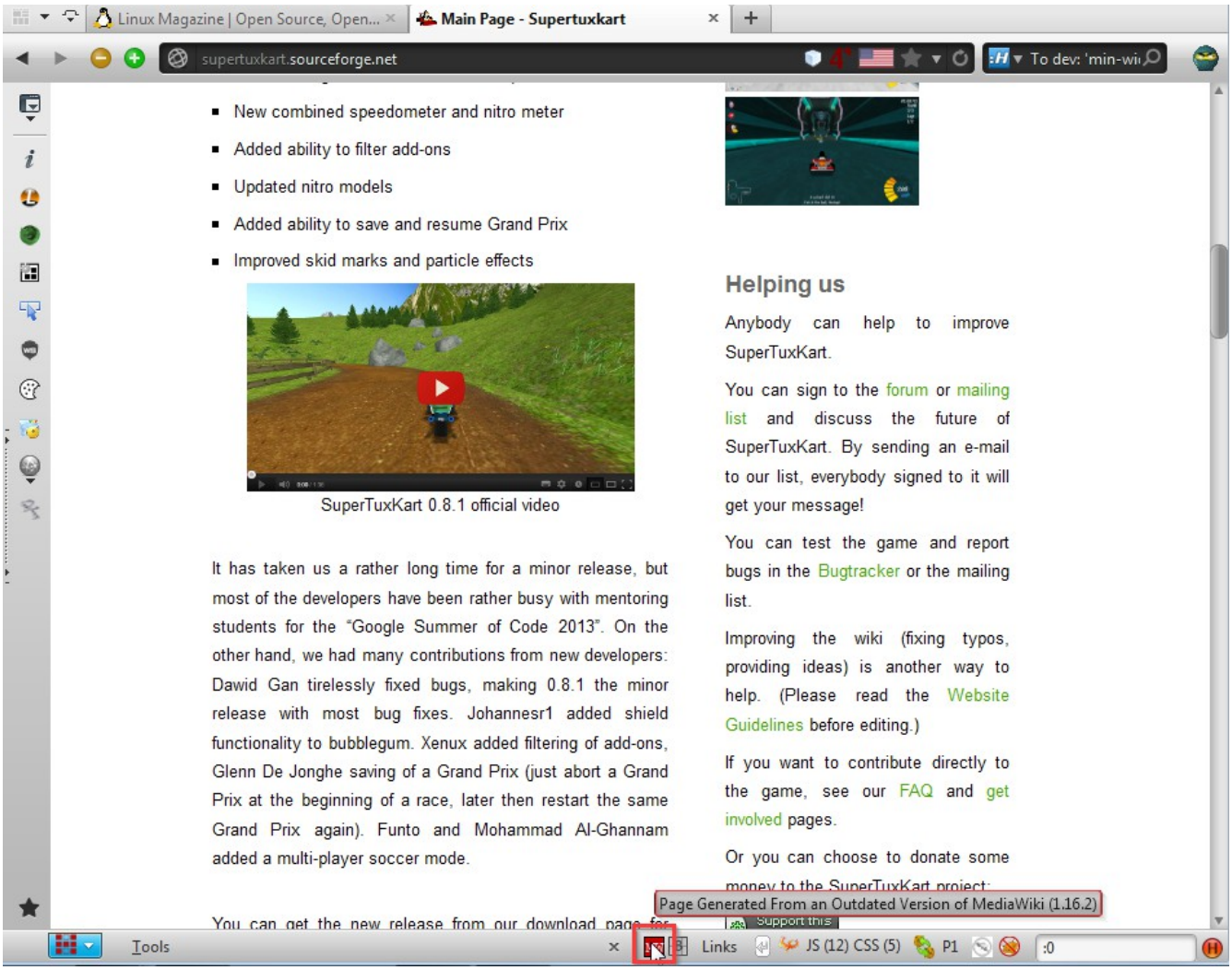

Linux Magazine | Open Source, Open...
Main Page - Supertuxkart
supertuxkart.sourceforge.net
To dev: 'min-wi
New combined speedometer and nitro meter
Added ability to filter add-ons
Updated nitro models
Added ability to save and resume Grand Prix
Improved skid marks and particle effects
SuperTuxKart 0.8.1 official video
It has taken us a rather long time for a minor release, but most of the developers have been rather busy with mentoring students for the "Google Summer of Code 2013". On the other hand, we had many contributions from new developers: Dawid Gan tirelessly fixed bugs, making 0.8.1 the minor release with most bug fixes. Johannesr1 added shield functionality to bubblegum. Xenux added filtering of add-ons, Glenn De Jonghe saving of a Grand Prix (just abort a Grand Prix at the beginning of a race, later then restart the same Grand Prix again). Funto and Mohammad Al-Ghannam added a multi-player soccer mode.
Helping us
Anybody can help to improve SuperTuxKart.
You can sign to the forum or mailing list and discuss the future of SuperTuxKart. By sending an e-mail to our list, everybody signed to it will get your message!
You can test the game and report bugs in the Bugtracker or the mailing list.
Improving the wiki (fixing typos, providing ideas) is another way to help. (Please read the Website Guidelines before editing.)
If you want to contribute directly to the game, see our FAQ and get involved pages.
Or you can choose to donate some
Page Generated From an Outdated Version of MediaWiki (1.16.2)
Tools
Links
JS (12) CSS (5)
P1

Figure 70: Supertuxkart website running Mediawiki v1.16.2

Wordpress v3.1 is running on linuxmag site:

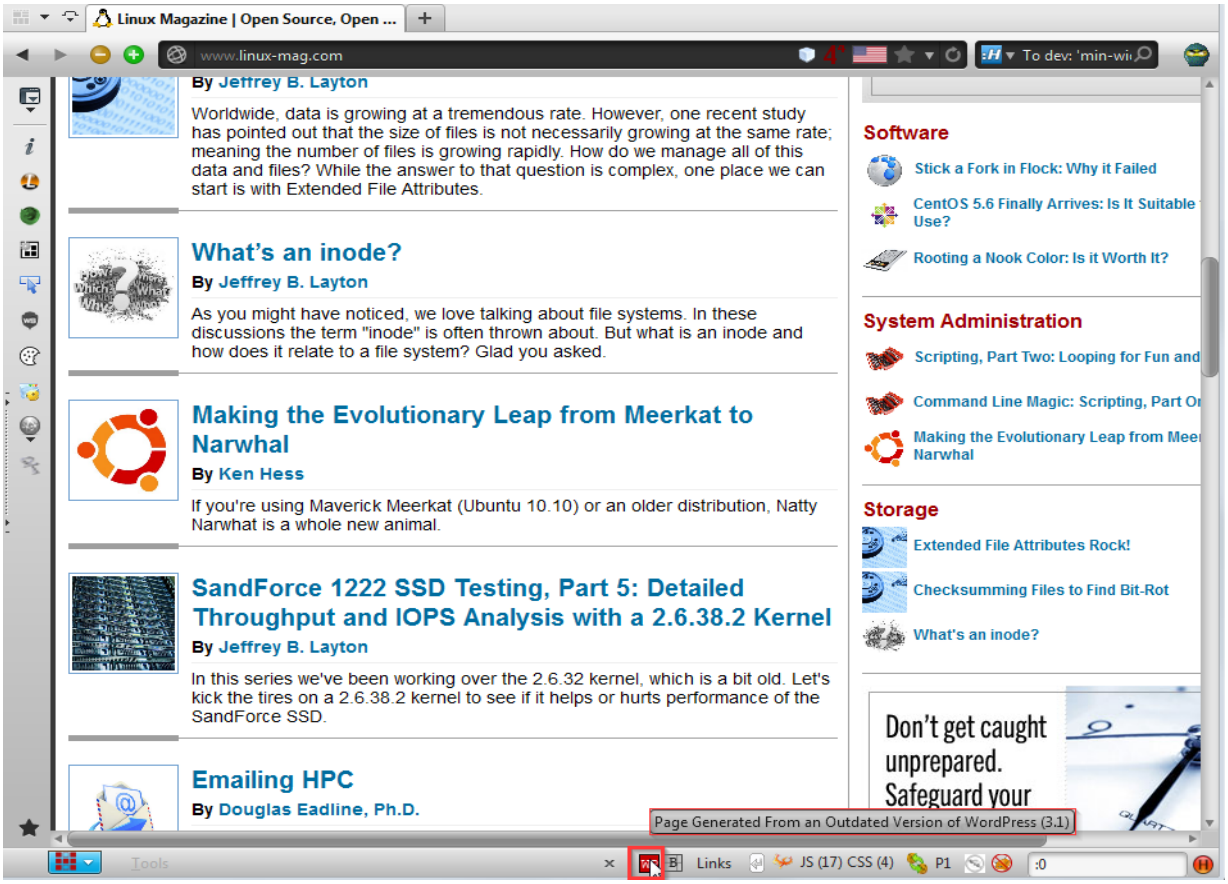

Linux Magazine | Open Source, Open ...
www.linux-mag.com
By Jeffrey B. Layton
Worldwide, data is growing at a tremendous rate. However, one recent study has pointed out that the size of files is not necessarily growing at the same rate; meaning the number of files is growing rapidly. How do we manage all of this data and files? While the answer to that question is complex, one place we can start is with Extended File Attributes.
What's an inode?
By Jeffrey B. Layton
As you might have noticed, we love talking about file systems. In these discussions the term "inode" is often thrown about. But what is an inode and how does it relate to a file system? Glad you asked.
Making the Evolutionary Leap from Meerkat to Narwhal
By Ken Hess
If you're using Maverick Meerkat (Ubuntu 10.10) or an older distribution, Natty Narwhat is a whole new animal.
SandForce 1222 SSD Testing, Part 5: Detailed Throughput and IOPS Analysis with a 2.6.38.2 Kernel
By Jeffrey B. Layton
In this series we've been working over the 2.6.32 kernel, which is a bit old. Let's kick the tires on a 2.6.38.2 kernel to see if it helps or hurts performance of the SandForce SSD.
Emailing HPC
By Douglas Eadline, Ph.D.
Software
Stick a Fork in Flock: Why it Failed
CentOS 5.6 Finally Arrives: Is It Suitable Use?
Rooting a Nook Color: Is it Worth It?
System Administration
Scripting, Part Two: Looping for Fun and
Command Line Magic: Scripting, Part O
Making the Evolutionary Leap from Mee Narwhal
Storage
Extended File Attributes Rock!
Checksumming Files to Find Bit-Rot
What's an inode?
Don't get caught unprepared. Safeguard your
Page Generated From an Outdated Version of WordPress (3.1)
Tools
Links
JS (17) CSS (4)
P1

Figure 71: Linuxmag running Wordpress v3.1

And all of this cms detection and version information is passive as it is not running any scans but uses the webpage source for detection, currently it can detect:

- WordPress versions prior to 3.8.1
- Joomla 1.0, 1.5, 1.6, and 1.7
- MediaWiki versions prior 1.19.12, 1.21.6, and 1.22.3
- vBulletin versions prior to 4.2.2
- TYPO3 version 4.6 and versions prior to 4.5
- Movable Type versions prior to 5.1561 and 5.2.9
- concrete5 versions prior to 5.6.2.1
- Zinnia versions prior 0.14
- Revive Adserver (formerly OpenX) versions price to 3.0.2
- WooFramework versions prior to 5.4.2

HconSTF has plethora of features for reconnaissance but one more quick one is to right click on a flag icon in url bar.

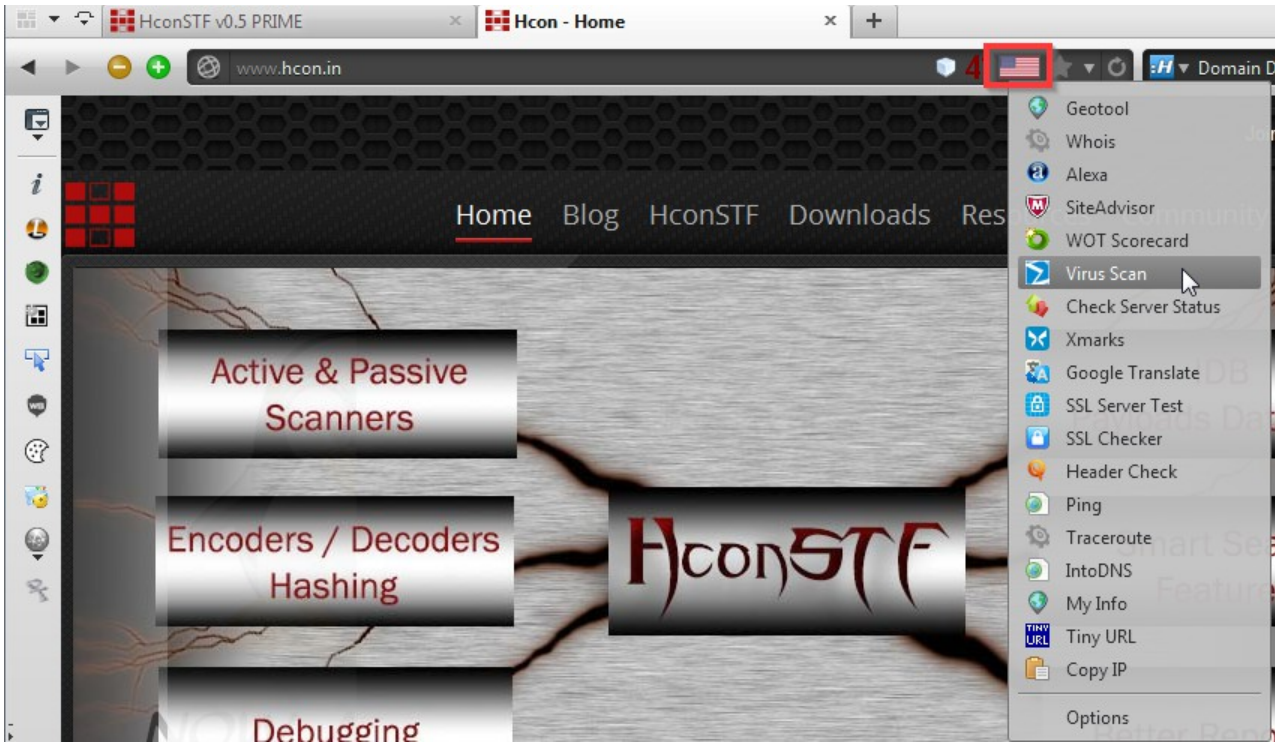


Figure 72: Running quick recon scans directly via url bar

To see more quick checks we can run on any target web site loaded in HconSTF

5.1.3 Metadata Analysis

In this age of content rich web 2.0, graphics are one of the important and most used data. and each image stores data about itself which is known as Metadata.

In terms of information gathering Metadata leads to lots of information, specially the images on web contains huge amount of information like, name of the device and model number from which the photo was taken, operating system of that device, if image is processed with any image editor, geographical location information from where the photo was taken, author name and more.

This information can be helpful in,

- Creating wordlist files
- Crafting specific mobile device exploits

- Social Engineering Attacks
- Geo-location information

Let us look at one of the recent trends on social media of taking "selfie" and see how much information it leaks. here we took a random photo from flickr.com, we right click on it and select 'View Image EXIF Data'

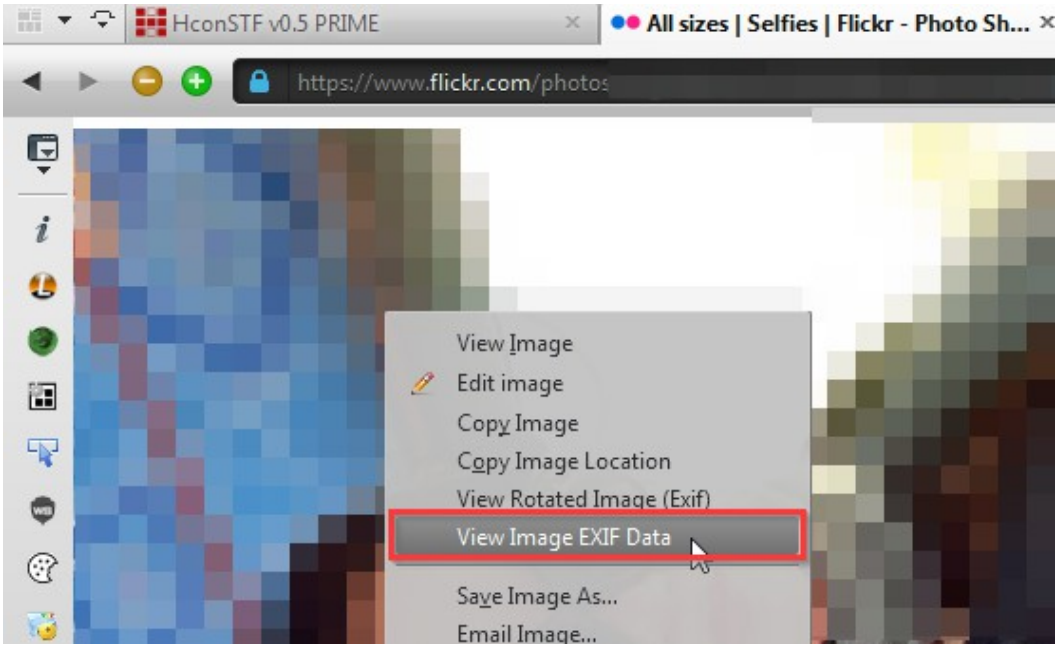


Figure 73: Viewing EXIF metadata

This photo stores too much of metadata we are specifically interested in,

Camera Make: Apple

Camera Model: iPhone 4S

Software / Firmware Version: 7.0.4

Last Modified Date/Time: 2014:02:10 10:01:33

Lens Make: Apple

Lens Model: iPhone 4S front camera 1.85mm f/2.4

GPS information: [REMOVED]

Google™ Maps

Yahoo!® Maps

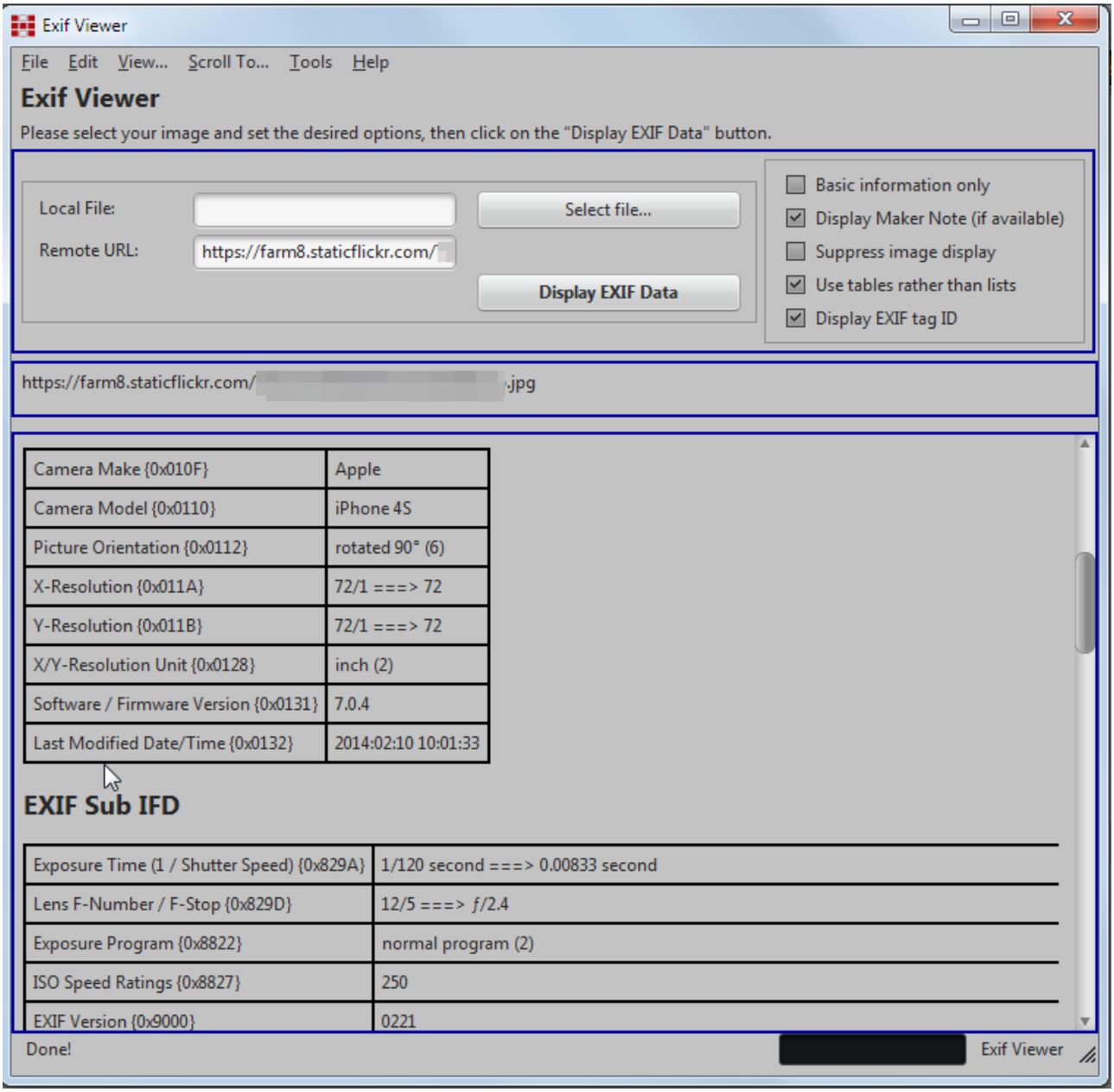
Bing® Maps

Mapquest®

Open KML data with Google™ Earth

Save KML data to file

Save KML data to file and open with Google™ Earth


Exif Viewer
File Edit View... Scroll To... Tools Help
Exif Viewer
Please select your image and set the desired options, then click on the "Display EXIF Data" button.
Local File:
Select file...
Remote URL:
https://farm8.staticflickr.com/
Display EXIF Data
Basic information only
Display Maker Note (if available)
Suppress image display
Use tables rather than lists
Display EXIF tag ID
https://farm8.staticflickr.com/ .jpg
Camera Make {0x010F} Apple
Camera Model {0x0110} iPhone 4S
Picture Orientation {0x0112} rotated 90° (6)
X-Resolution {0x011A} 72/1 ===> 72
Y-Resolution {0x011B} 72/1 ===> 72
X/Y-Resolution Unit {0x0128} inch (2)
Software / Firmware Version {0x0131} 7.0.4
Last Modified Date/Time {0x0132} 2014:02:10 10:01:33
EXIF Sub IFD
Exposure Time (1 / Shutter Speed) {0x829A} 1/120 second ===> 0.00833 second
Lens F-Number / F-Stop {0x829D} 12/5 ===> f/2.4
Exposure Program {0x8822} normal program (2)
ISO Speed Ratings {0x8827} 250
EXIF Version {0x9000} 0221
Done!
Exif Viewer

It also gives us Geo location information but for purpose of this we removed it, via that we can open that location in many online maps services and even store it to .kml file for later use.

We can also select an external image file to view its EXIF data.

5.2 Testing for Vulnerabilities

5.2.1 Cross Site Scripting (XSS)

XSS stands for Cross Site Scripting, it is an attack which is type of injection attack which injects JavaScript and executes in user's web client which can do all the things which we can do as a user by JavaScript like modifying the page content, stealing user cookies in browser, some more advanced attack includes XSS worm, Puppetnet (with beef), XSS shell and much more.

XSS are categories in 3 types,

- Reflected XSS (non-persistent)
- Stored XSS (persistent)
- DOM based XSS

We will going to use HconSTF on DVWA as target site for finding reflected XSS vulnerability.

We start with XSS scanner from HconSTF

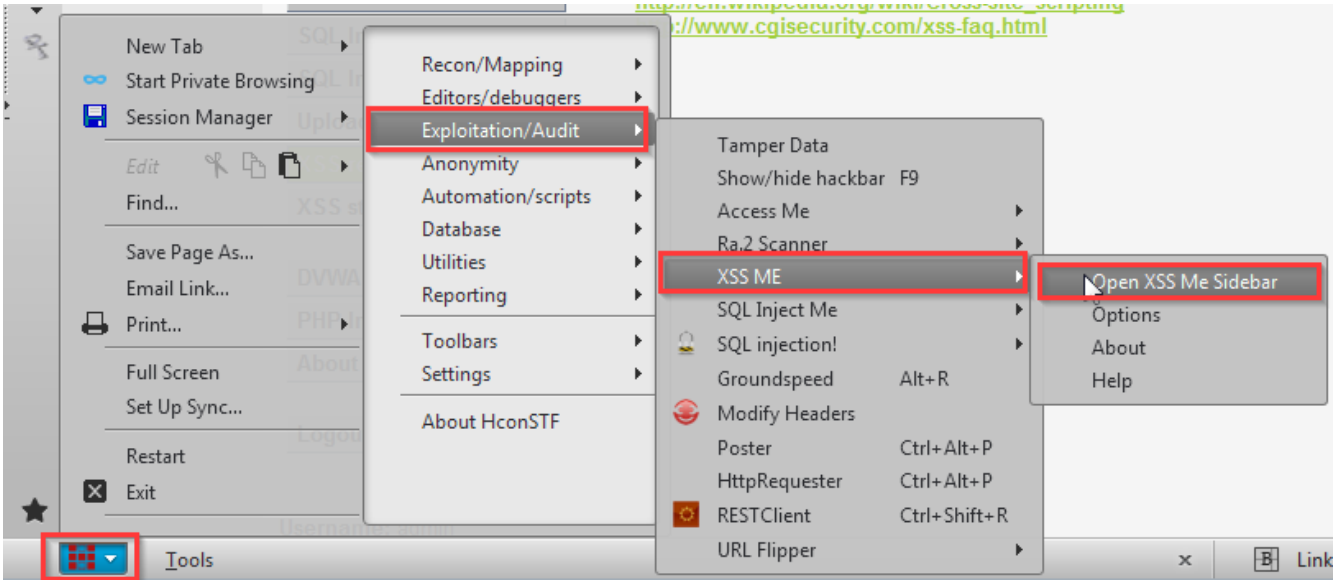


Figure 74: Starting XSS scanner from HconSTF

Goto Hmenu → Exploitation/Audit → XSS ME → Open XSS Me Sidebar.

XSS scanner shows fields on the page which can be tested against known attack payloads and provides option to test all fields against all attacks or only using top attacks.

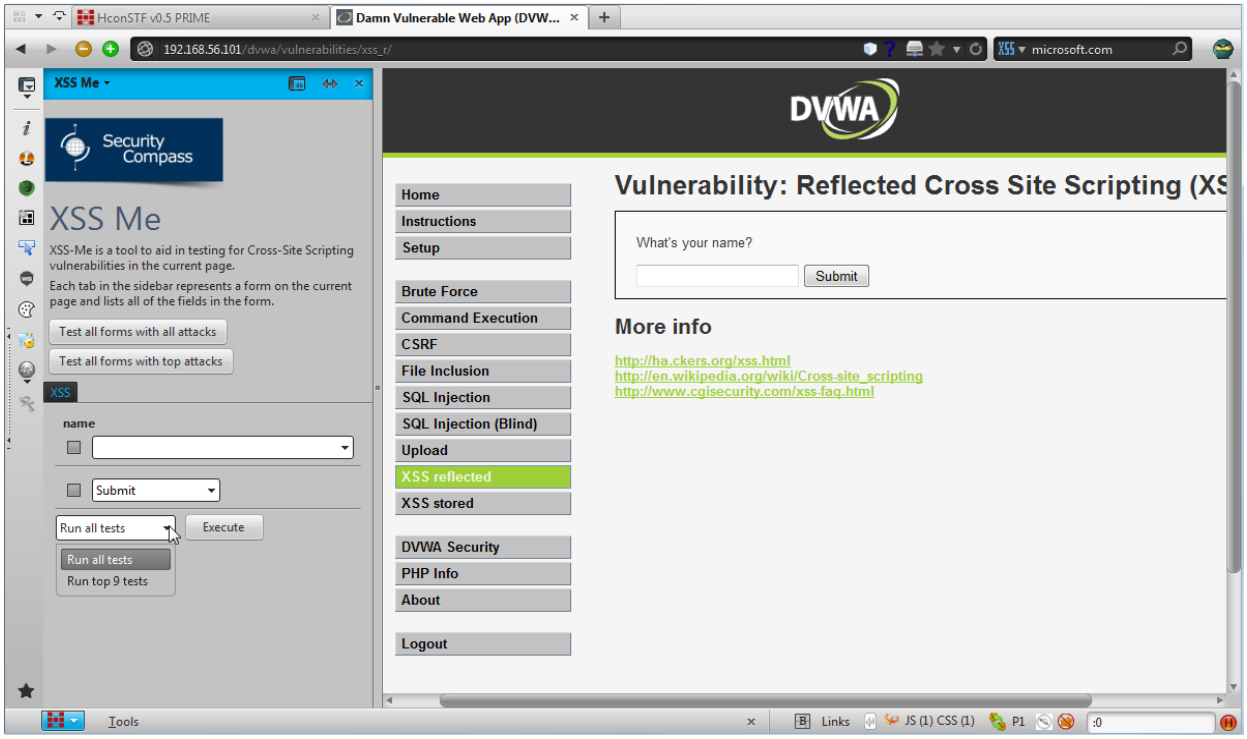


Figure 75: XSS Me sidebar

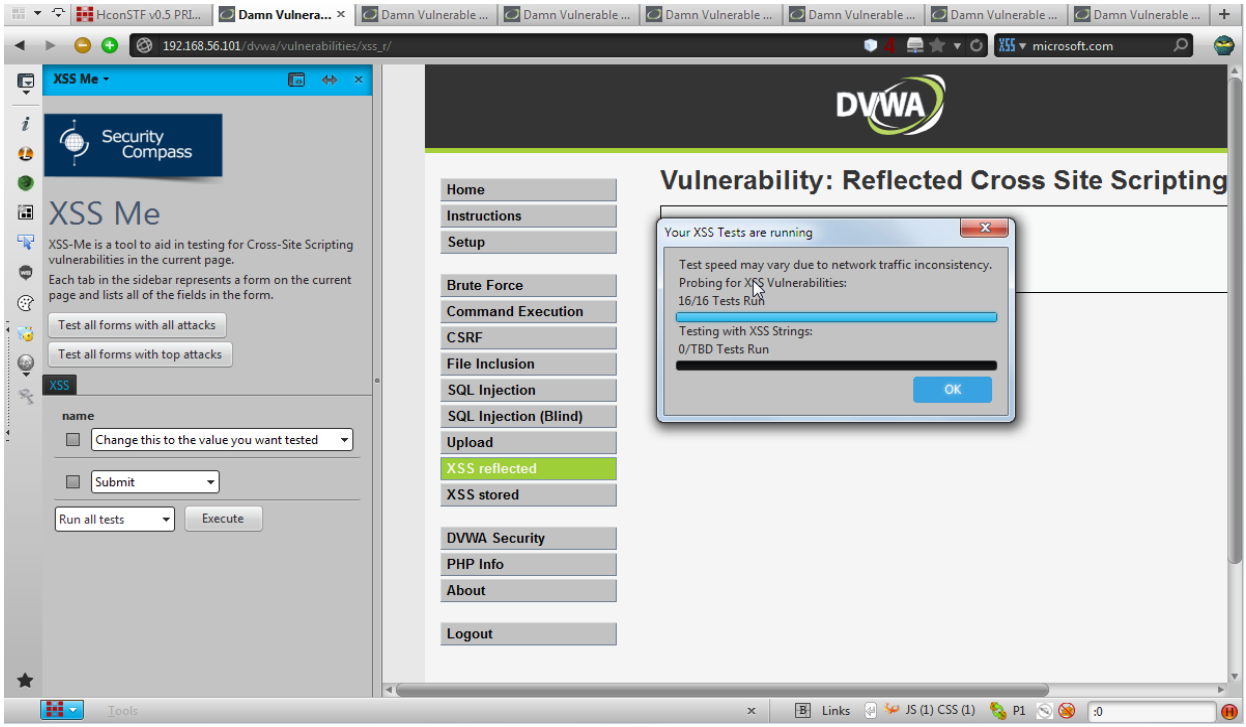


Figure 76: Scanning for vulnerabilities

Once the scanner completes testing, we will be presented with a simple HTML report with worked XSS attacks attempts, based on the results we got from the scanner one of the attack string which is successfully executed was <script>document.vulnerable=true</script>

We can use that and verify the vulnerability by slightly modifying the attack string to reflect in browser <script>alert(document.cookie);</script>

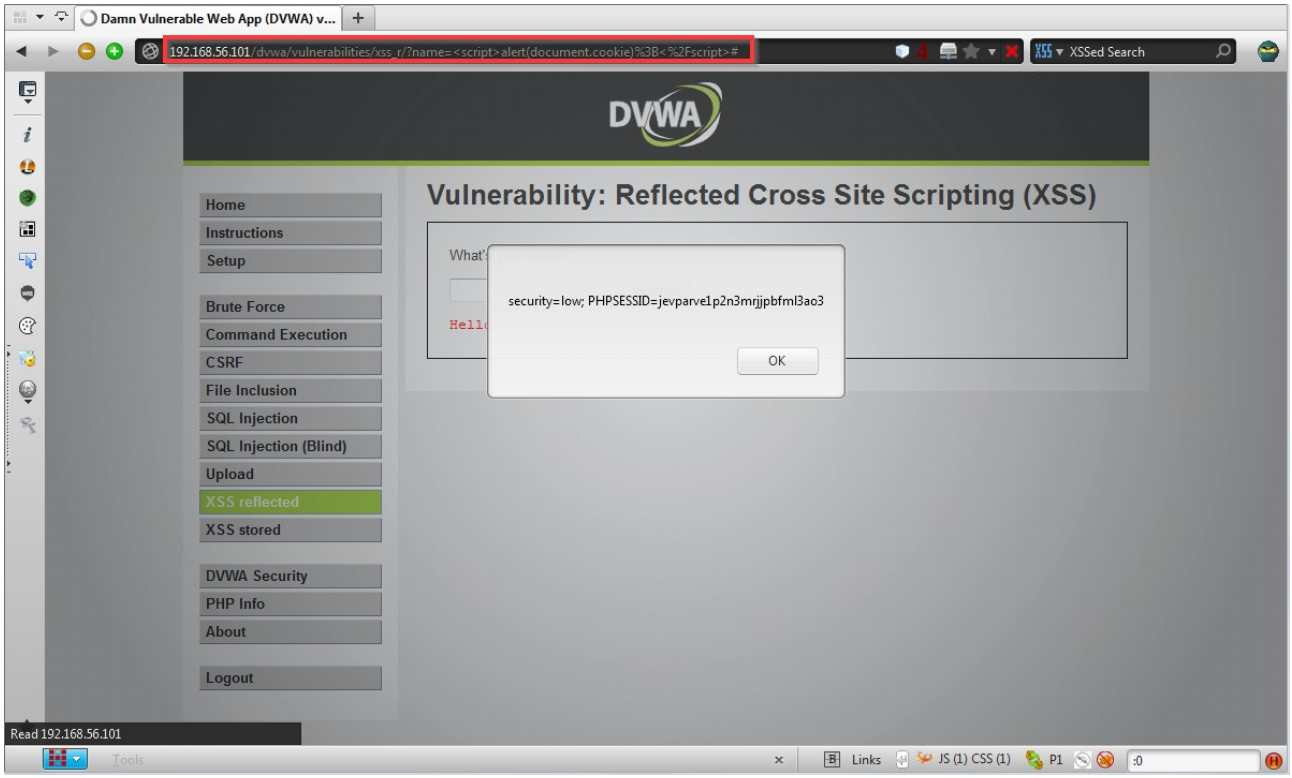


Figure 77: Manually verifying vulnerability

As it executed and reflected the JavaScript and showed cookies in alert box, by this we can verify the detected XSS.

By default the included XSS attack payloads only detects XSS vulnerability, for actual exploitation we can use payloads from IDB or craft our own and import it into the scanner.

goto Hmenu → Exploitation/Audit → XSS ME → Options

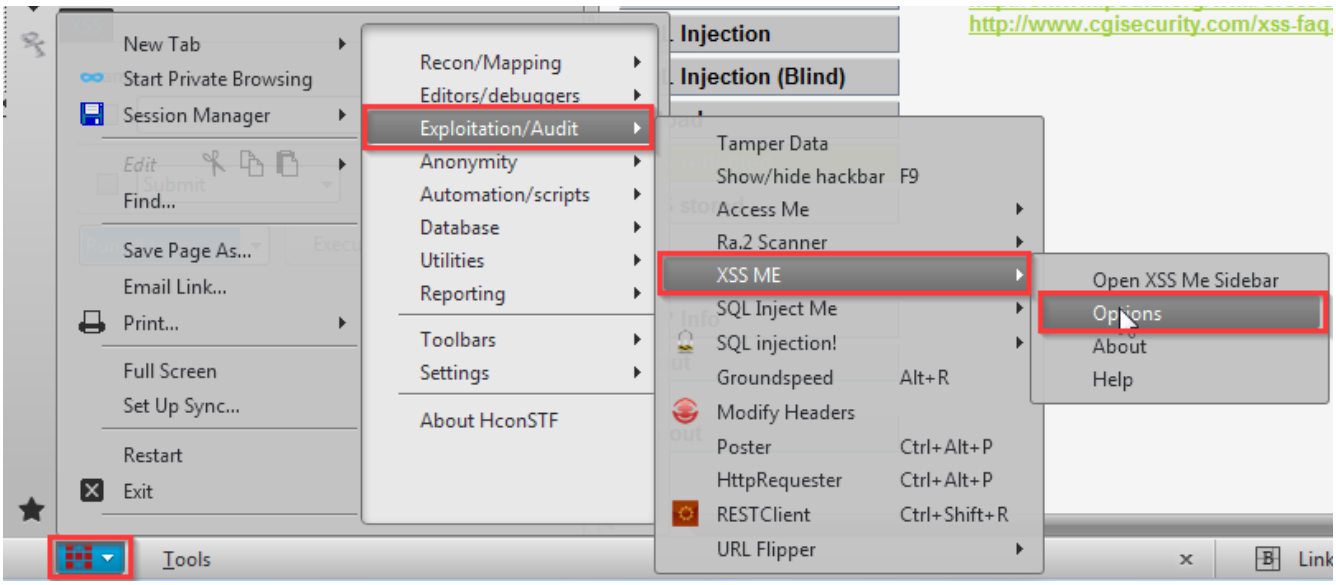


Figure 78: Configuring XSS scanner

In its options window we can import and export attack payload strings, configure delay between each attack execution and more.

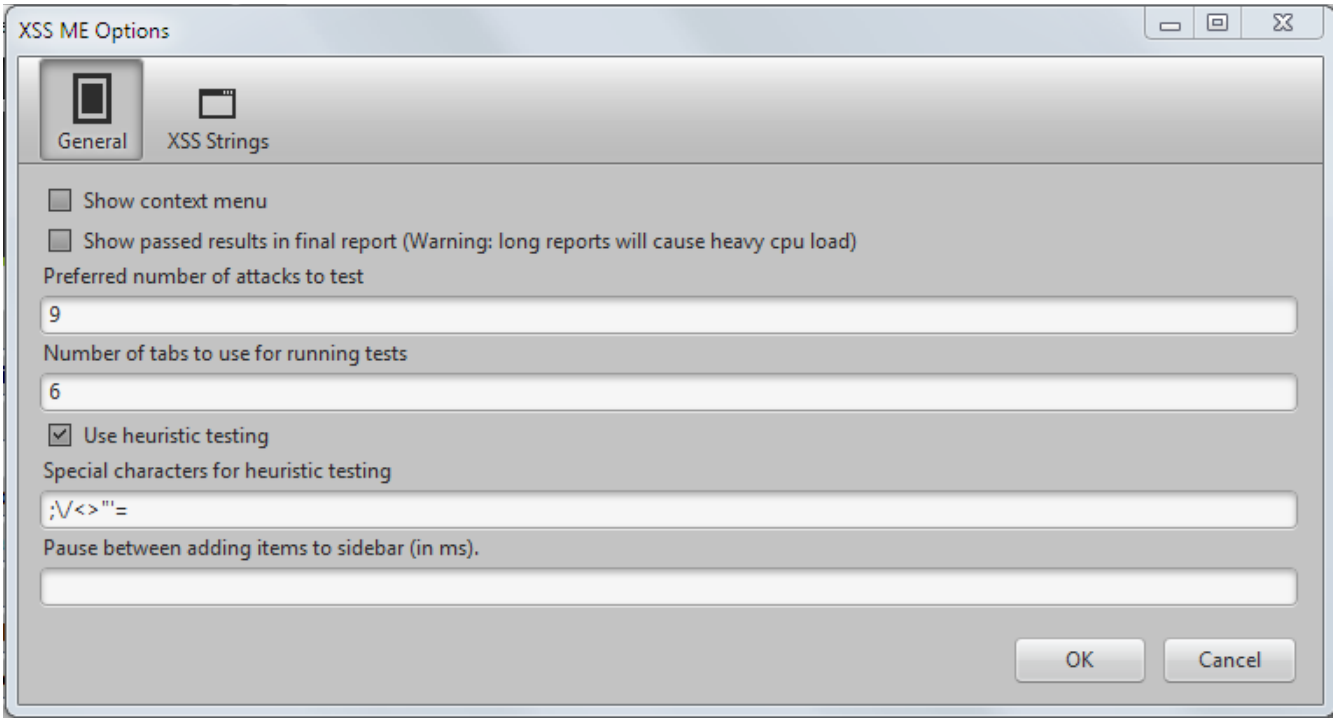


Figure 79: XSS scanner configuration window

IDB in HconSTF comes with huge database of XSS attack payloads for XSSme tool and Search XSS tool which can be found at HconSTFPortable/Extras/IDB

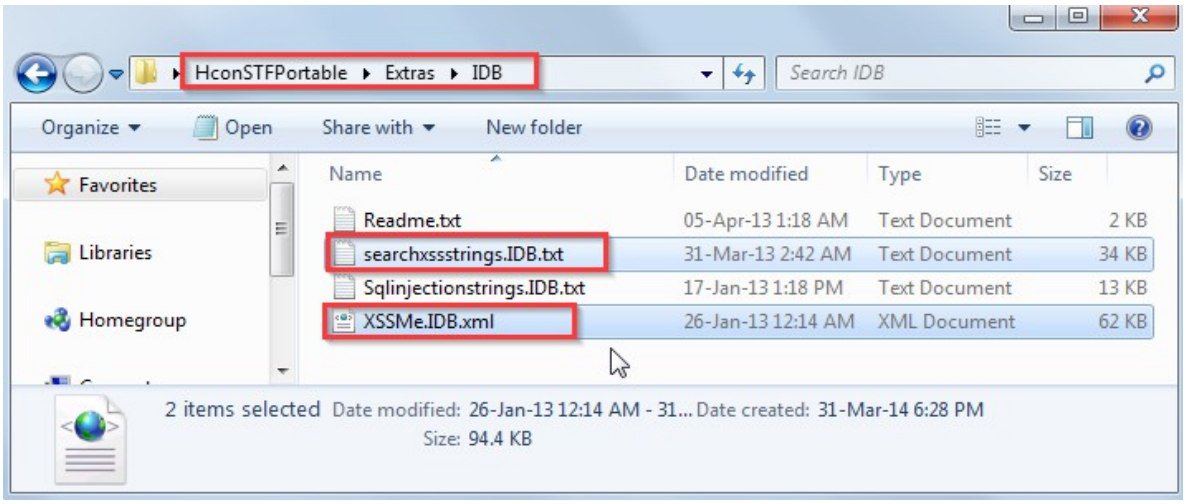


Figure 80: Importable XSS strings from IDB

While using this much bigger database to scan our target, it will going to use more system resources but can reduce lot of work by detecting more XSS vulnerabilities.

WebUI has 3 more XSS scanners which can be used for scanning target.

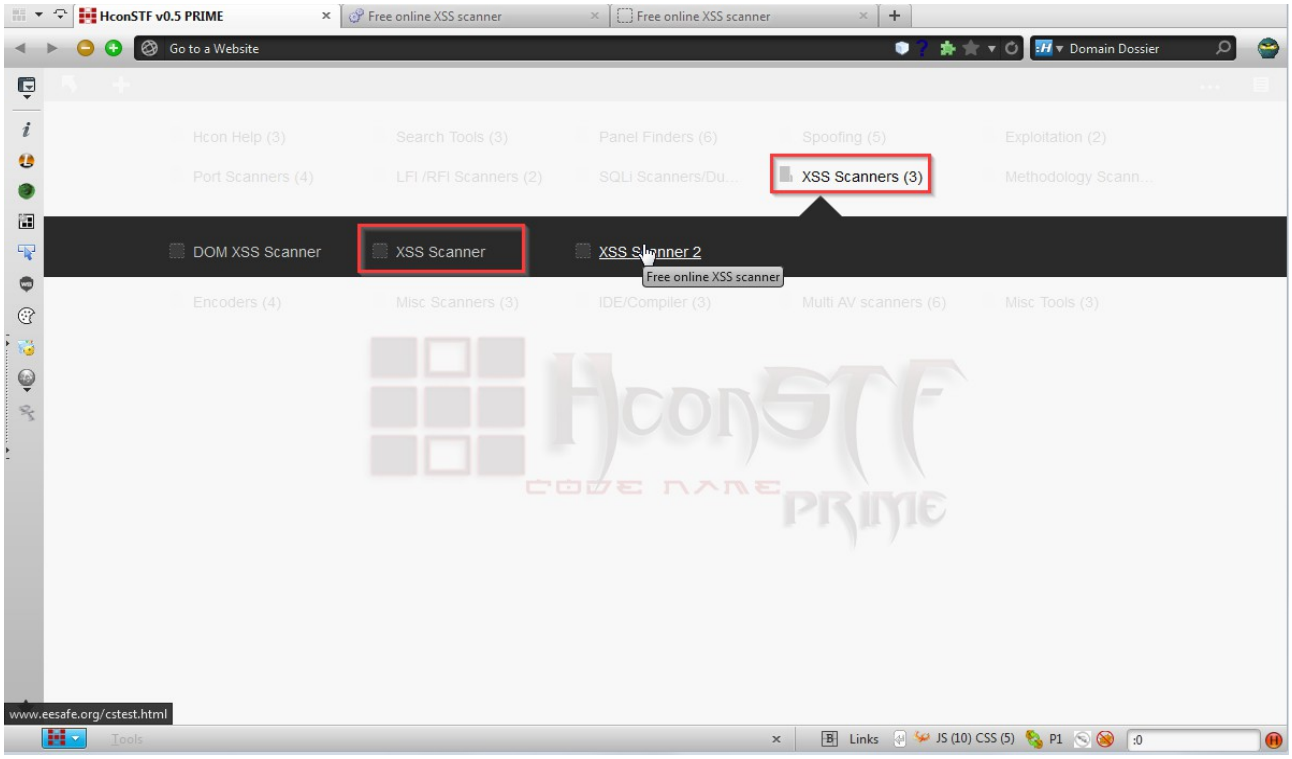


Figure 81: XSS scanners in WebUI

First one is for DOM based XSS scanning and the other two are for Reflected XSS scanning, we will going to use reflected XSS scanner as seen in the figure below.

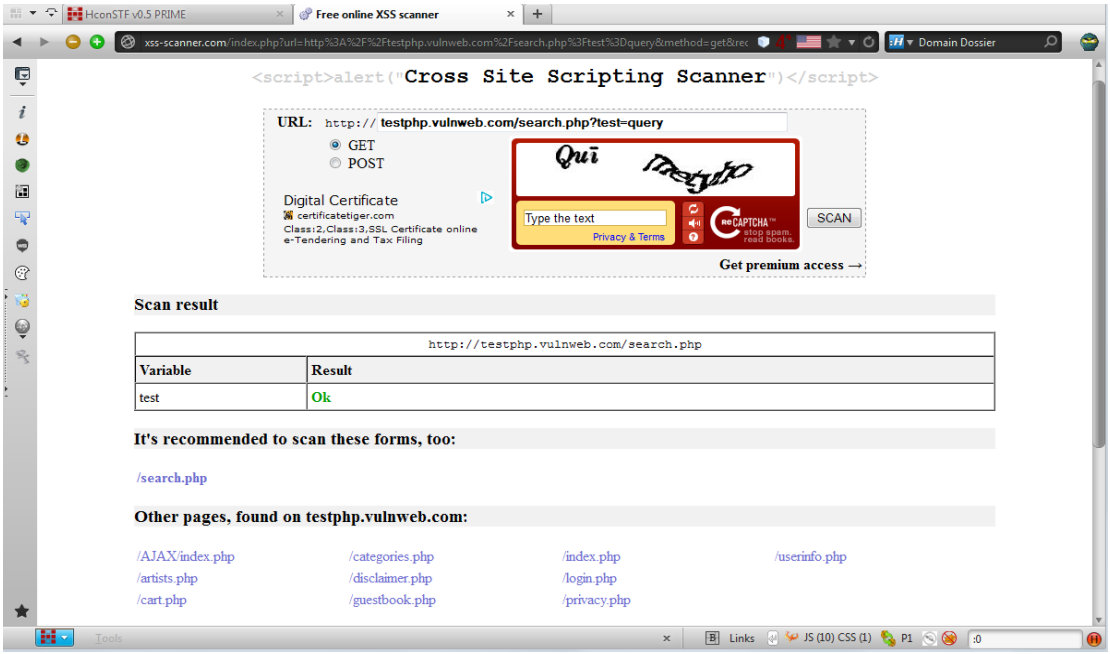


Figure 82: Running XSS scanner from WebUI

We can also check for any past XSS vulnerabilities on the site.

Enter the domain name in Search Aggregator → Search Exploits → XSSed Search

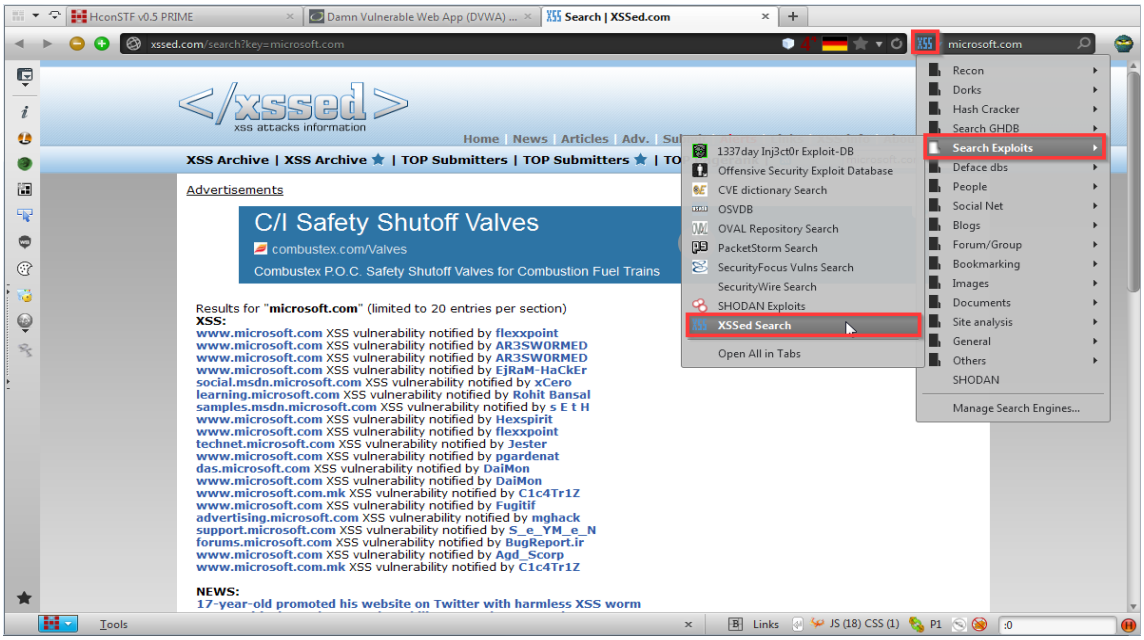


Figure 83: Reported XSS vulnerabilities for microsoft.com

For this example we searched for microsoft.com and it listed all the reported XSS attacks. This kind of site comes handy for gathering new attack vectors, and for a known vulnerable page on a specific target we are testing and in some cases even if the attack is reported the site doesn't patch it.

5.2.2 SQL Injection (SQLi)

We will going to use HconSTF on DVWA as target site for finding sql injection vulnerability with some what the same process. first we start SQLi scanner from HconSTF,

goto Hmenu → Exploitation/Audit → SQL Inject Me → Open SQL Inject Me Sidebar

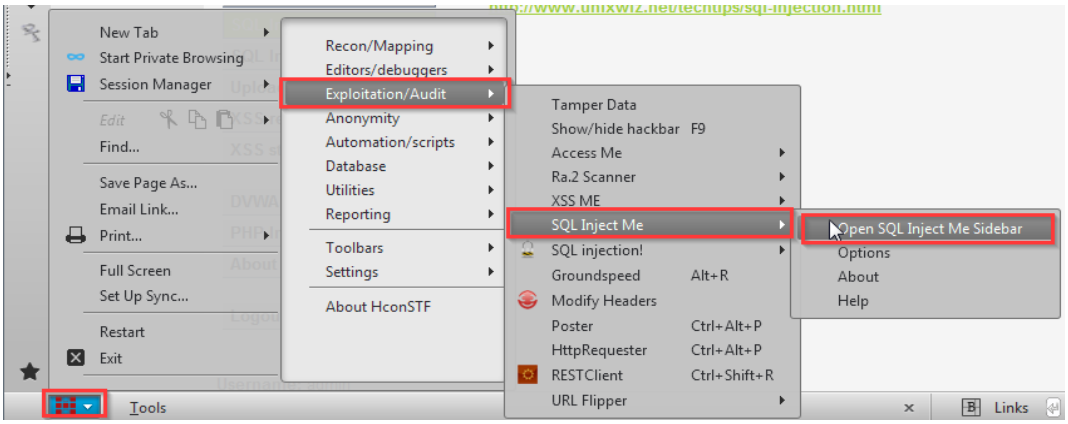


Figure 84: SQL injection scanner in HconSTF

SQLi scanner shows fields on the page which can be tested against known attack payloads and provides option to test all fields against all attacks or only top attacks.

Figure 85: SQL Inject Me sidebar

Scanning for vulnerabilities with SQL inject me scanner

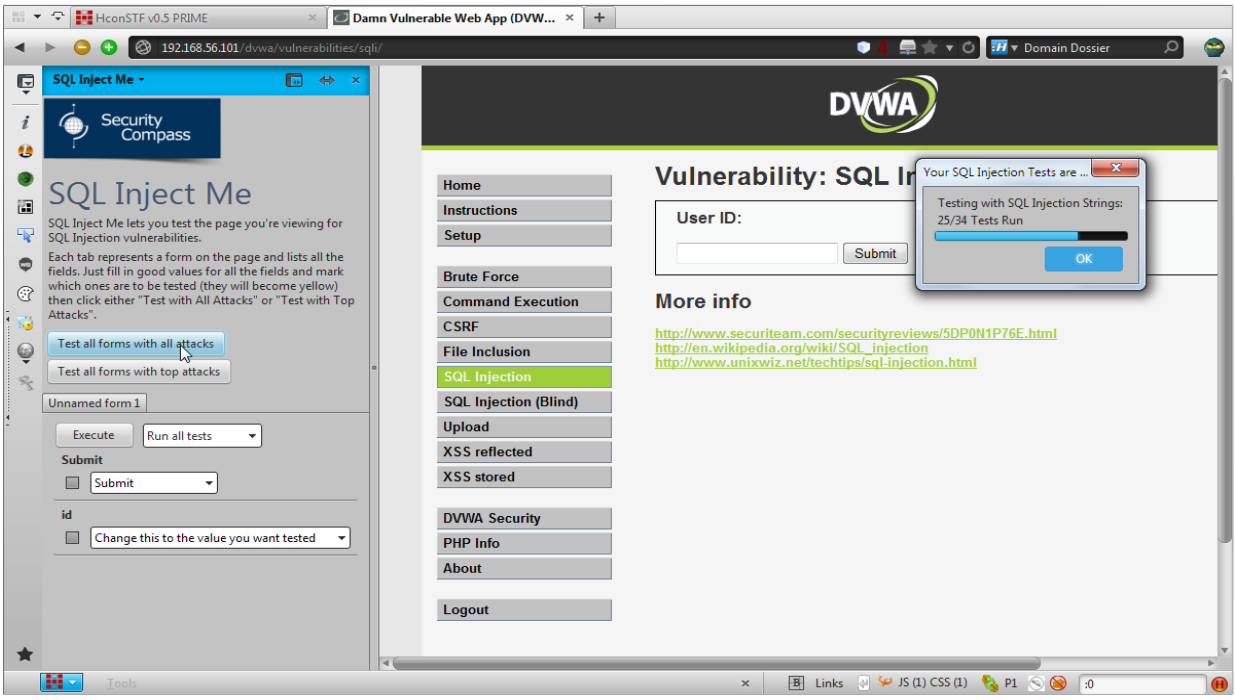


Figure 86: SQL injection scanner running

A scan report will be presented with worked SQL Injection attacks attempts. Based on the results we got from the scanner, one of the attack string which is successfully executed was ' or 1=1--

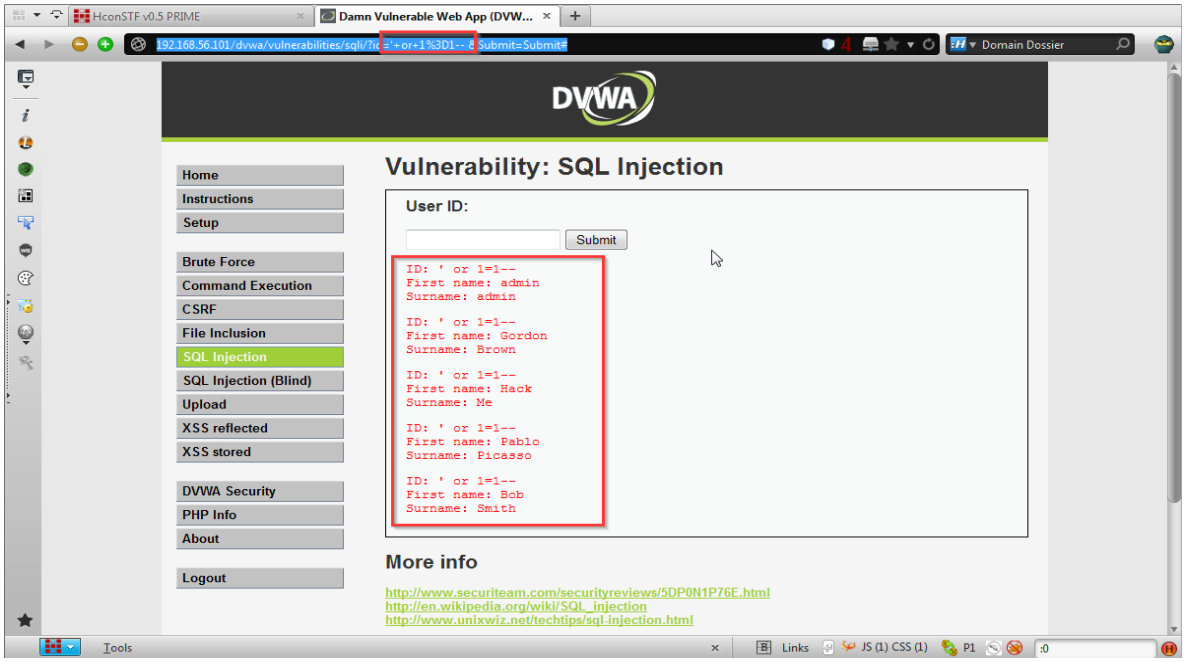


Figure 87: Successfully executed SQL injection attack

We can use that and verify the vulnerability by slightly modifying the url string to: http://192.168.56.101/dvwa/vulnerabilities/sqli/?id=%27+or+1%3D1--%20&Submit=Submit

as in figure 87 its executed and dumped some entries from the database, by this we can verify the detected SQL Injection.

By default the included SQL injection attack payloads are limited and detects injection vulnerability on few database types, for actual exploitation we can use payloads from IDB or craft our own and import it into the scanner.

goto Hmenu → Exploitation/Audit → SQL Inject Me → Options

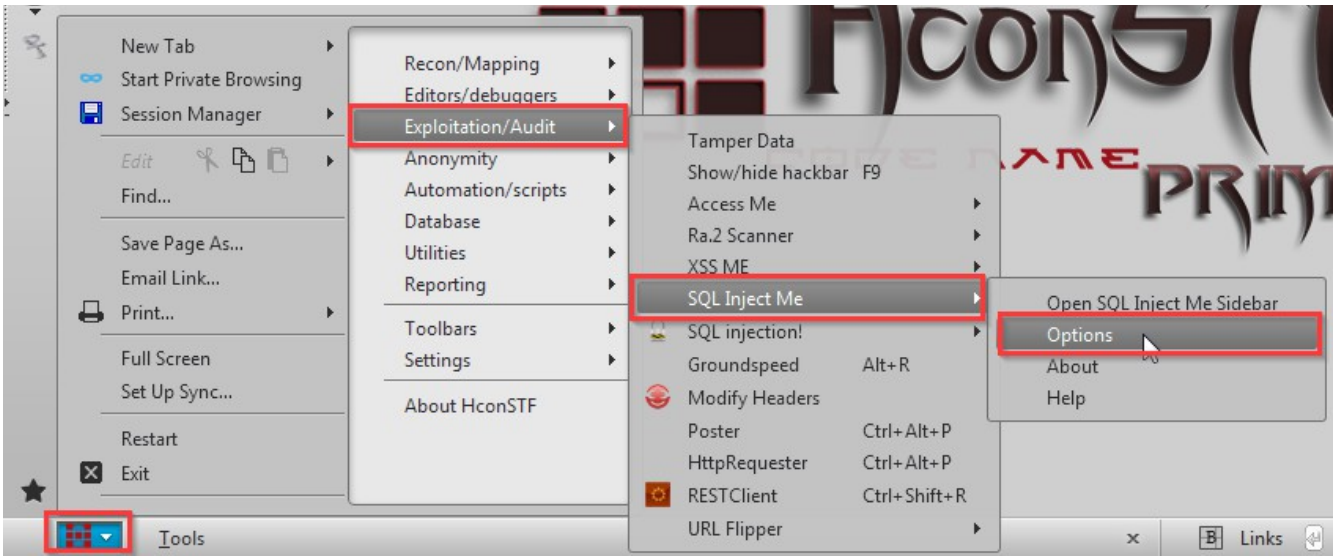


Figure 88: SQL inject me options

In its options window we can import and export attack payload strings and error status strings, configure delay between each attack execution and more.

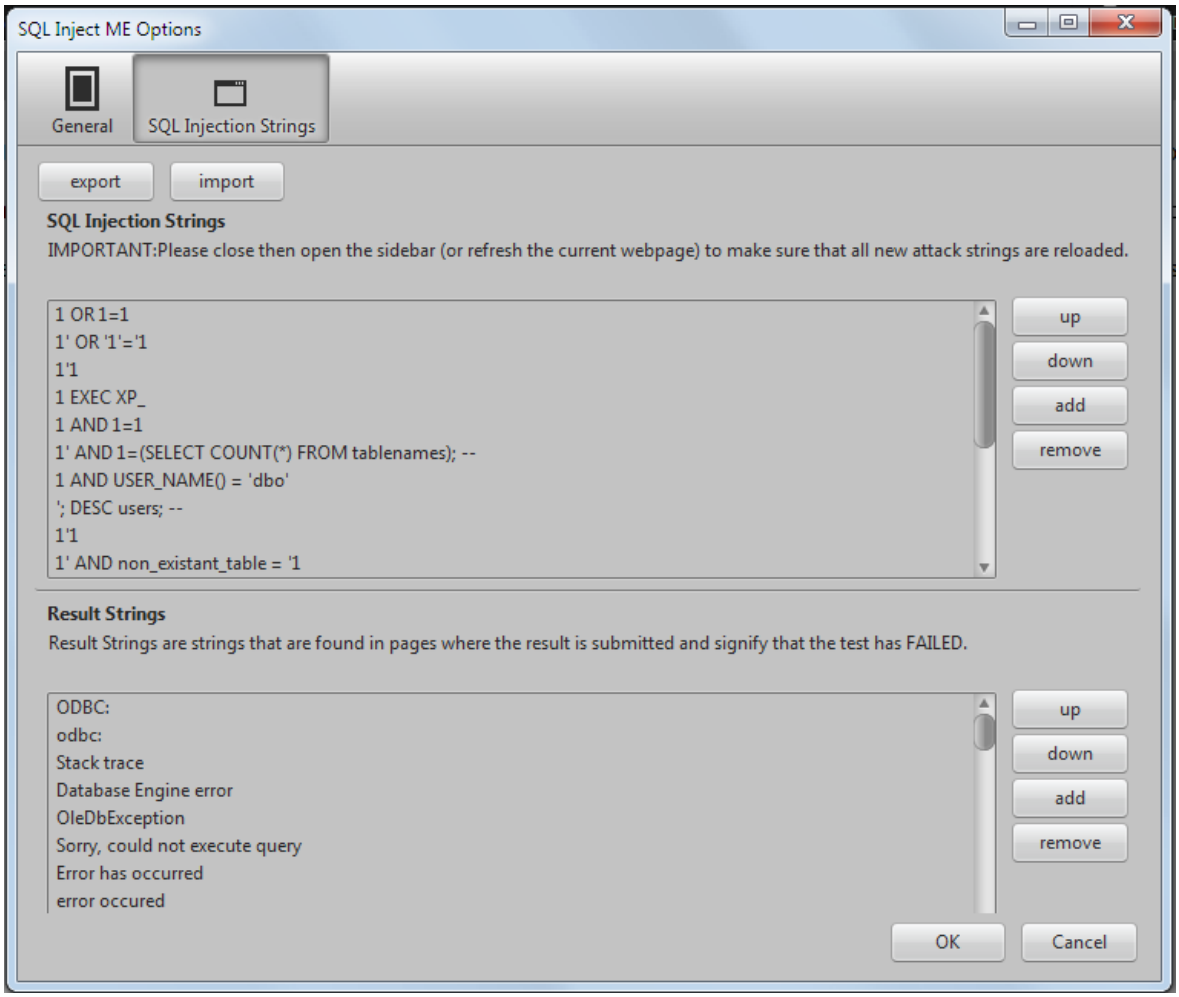


Figure 89: Importing/exporting detection strings

IDB in HconSTF comes with huge database of SQL Injection attack payloads for SQL Inject Me tool, which can be found at HconSTFPortable/Extras/IDB directory

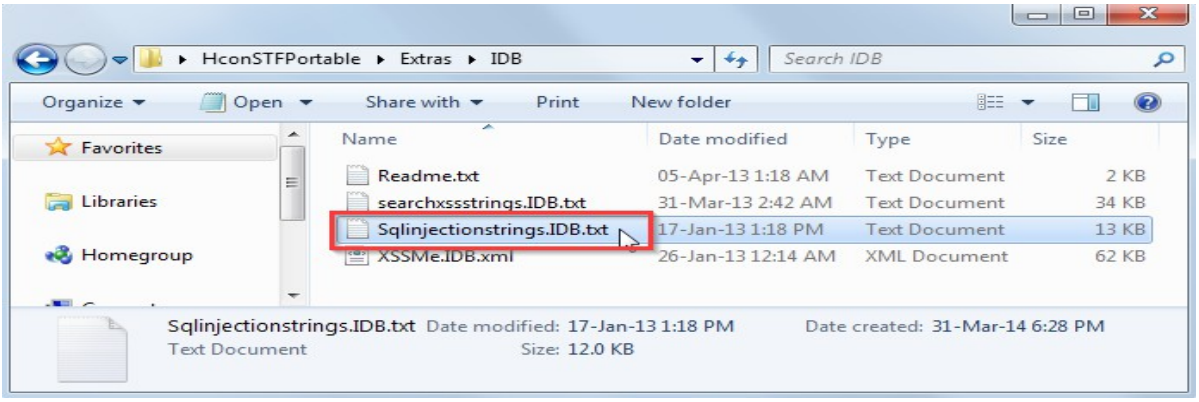


Figure 90: importable SQLi strings from IDB

While using this much bigger database to scan our target, it will going to use more system resources but can reduce lot of work by detecting more SQL Injection vulnerabilities.

WebUI has 3 more SQL injection scanners which can be used for scanning target.

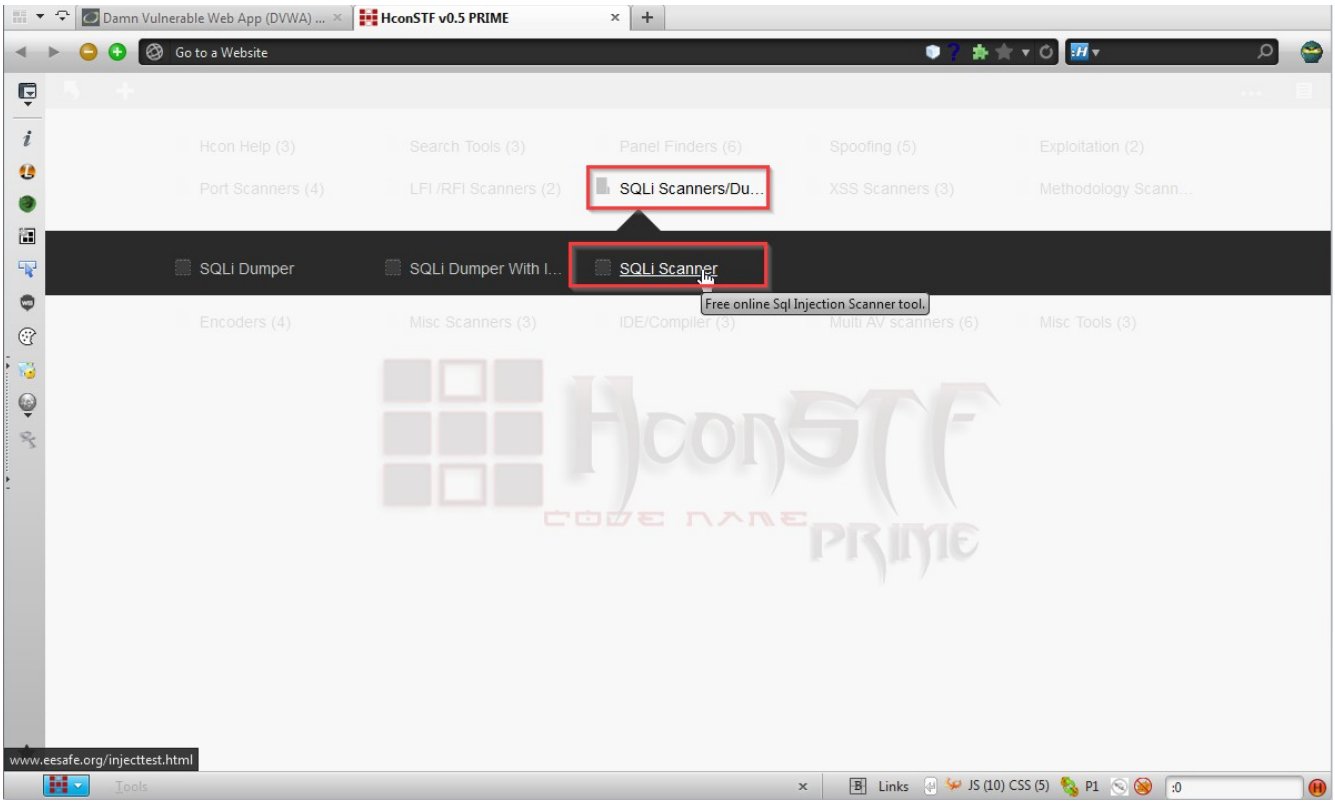


Figure 91: SQL injection scanners in WebUI

This scanners detects if the url variable is vulnerable to injection or not.

5.2.3 File Upload Vulnerability

Many web apps/sites has option of uploading any type of file in context to where it is available. like in forums for uploading avatar images, uploading small attachment files, as such many sites has documents uploading capabilities.

This feature of sites must be tested against file upload vulnerability of bypassing access controls and direct object referencing, this can lead to complete server compromise.

For demonstration of this attack we will use DVWA's upload file page and try to bypass the security controls in place. We will going to use b374k mini webshell as malicious file to be upload so rename its file extension to .txt (file name injsh.txt)

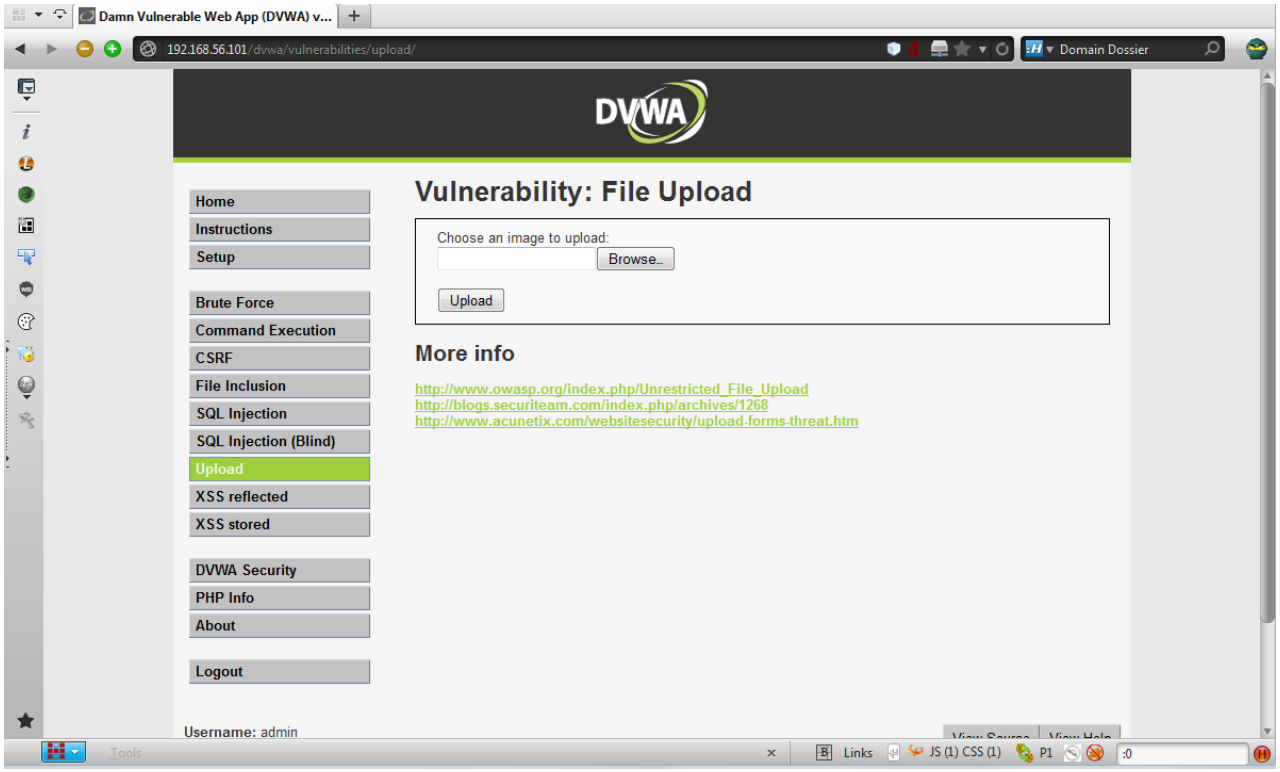


Figure 92: DVWA - upload file page

Start tamper data tool for intercepting web requests by All sidebar panels button → Tamper Data

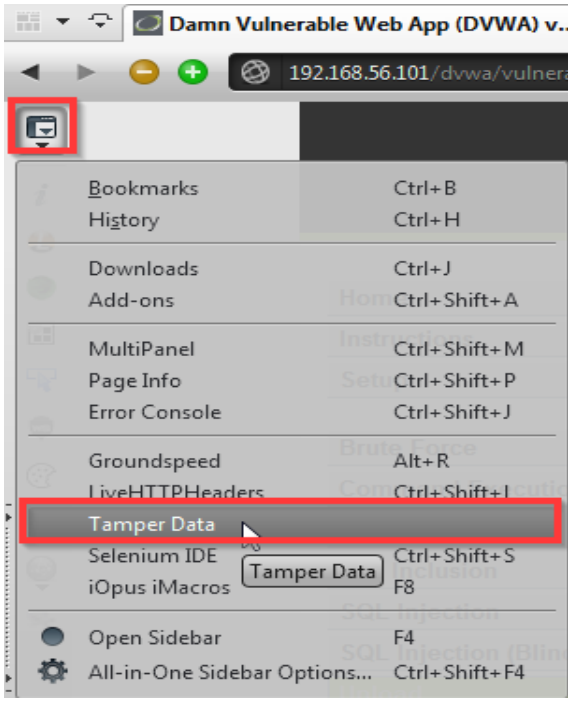


Figure 93: Open Tamper data in sidebar

click on 'Start Tamper'

Figure 94: Starting Tamper data for intercepting web traffic

Now browse for the file to upload, select it and upload it.

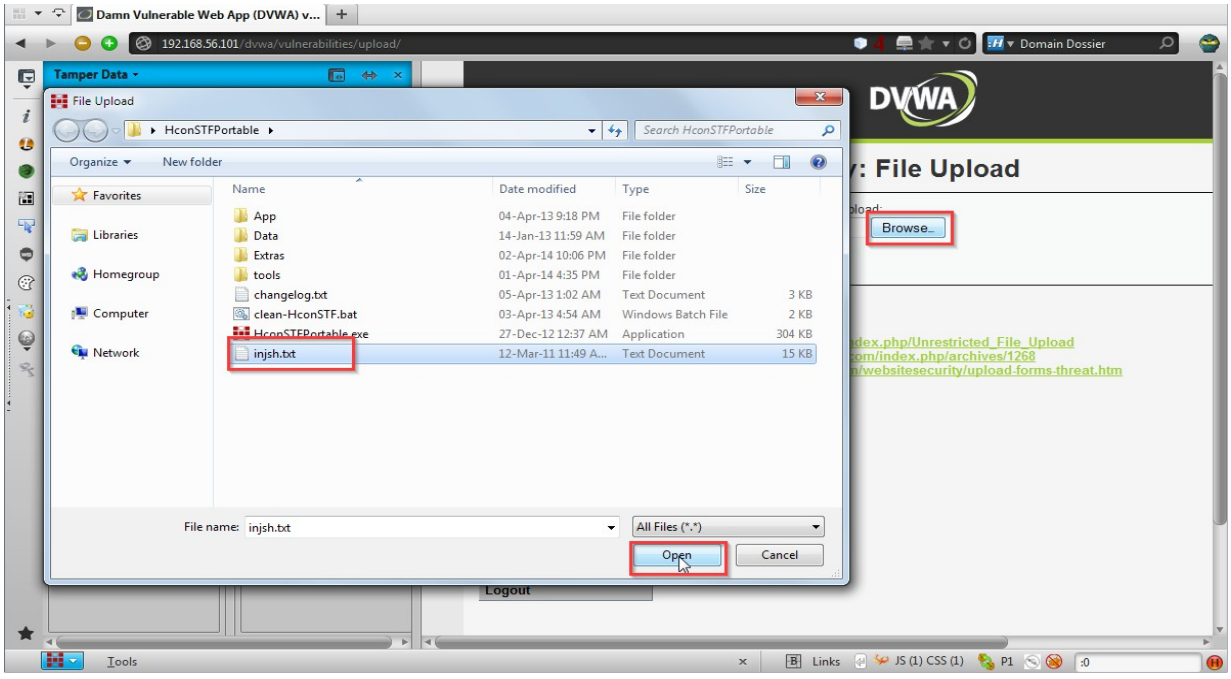


Figure 95: Select and upload file

Make sure that the file we are trying to upload which is a webshell is renamed with acceptable file extension for the site like .img, .txt etc. Click on upload button and it will ask us for tamer request or not, click on 'Tamper'

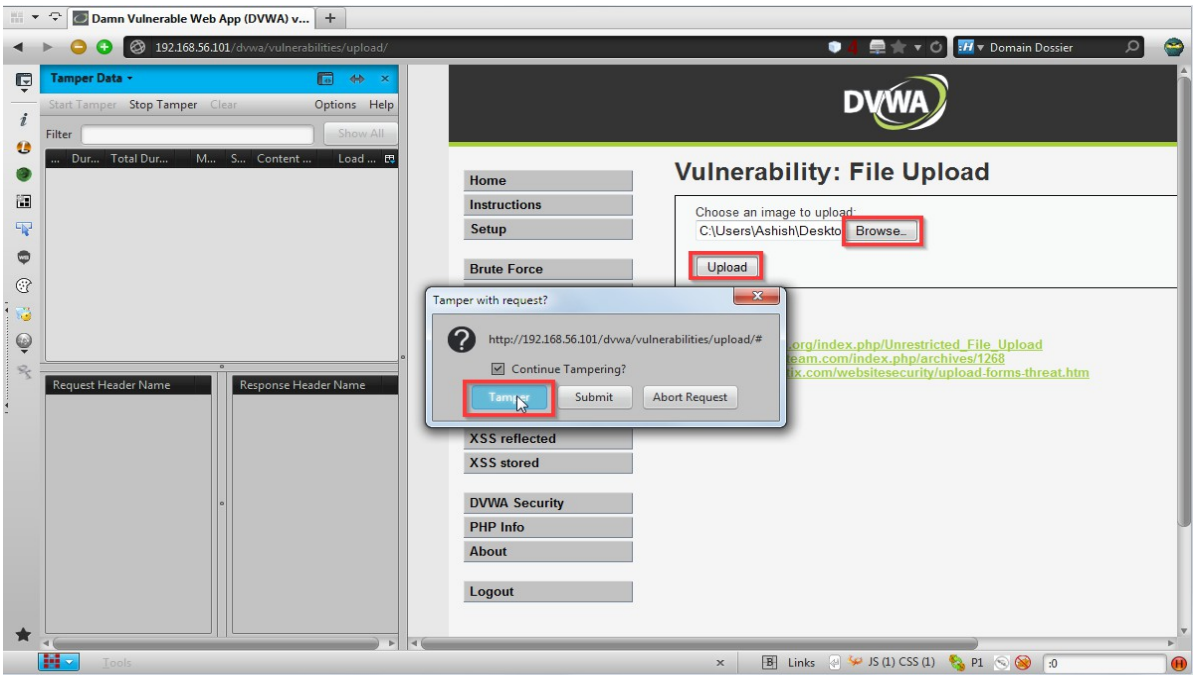


Figure 96: Tampering the upload request

In tamper popup window edit the file's extension from .txt to original .php and click 'ok'

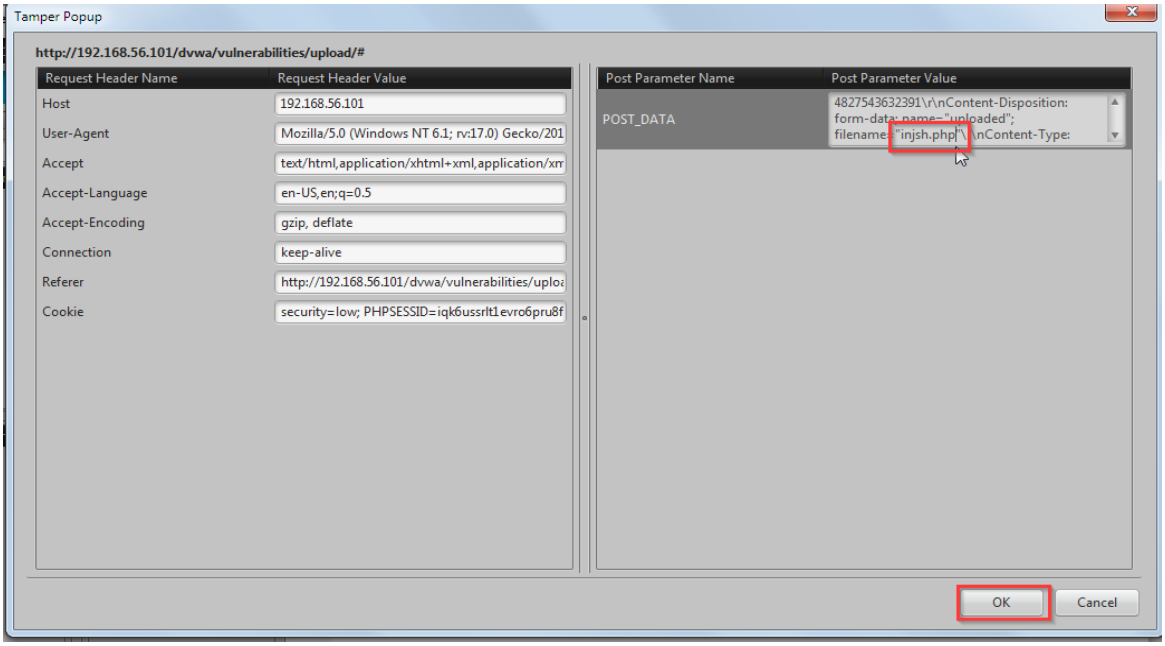


Figure 97: Change the file extension from txt to php

For the next tamper request untick 'Continue Tampering?' and click on 'Submit'

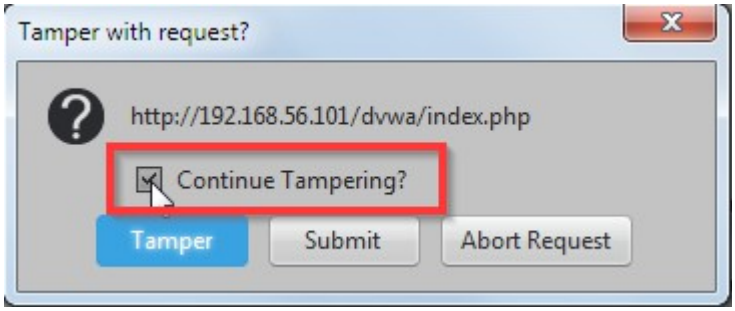


Figure 98: Discontinue tampering requests

DVWA responses on the upload page that the file upload is successful and gives the path to the uploaded file.

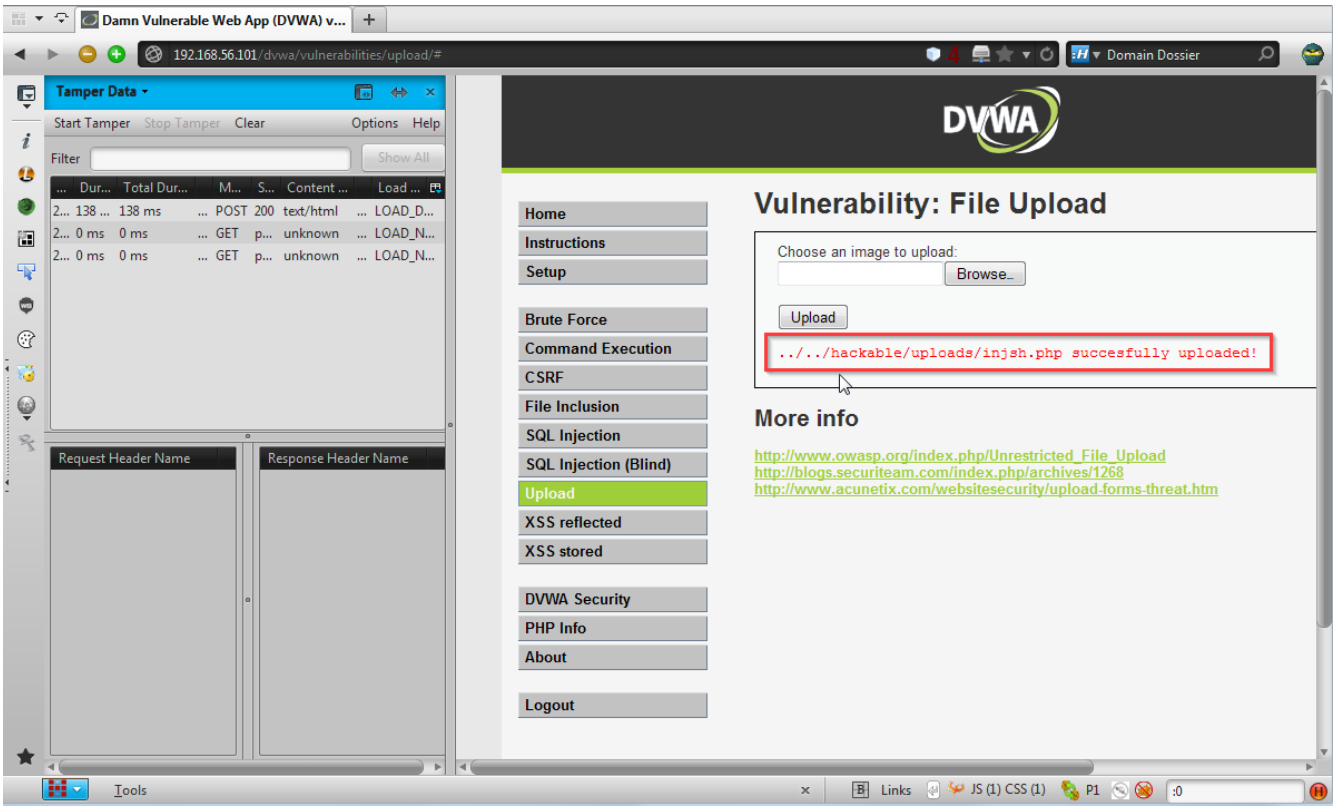


Figure 99: File uploaded

lets try to access the path at:

http://192.168.56.101/dvwa/hackable/uploads/injsh.php

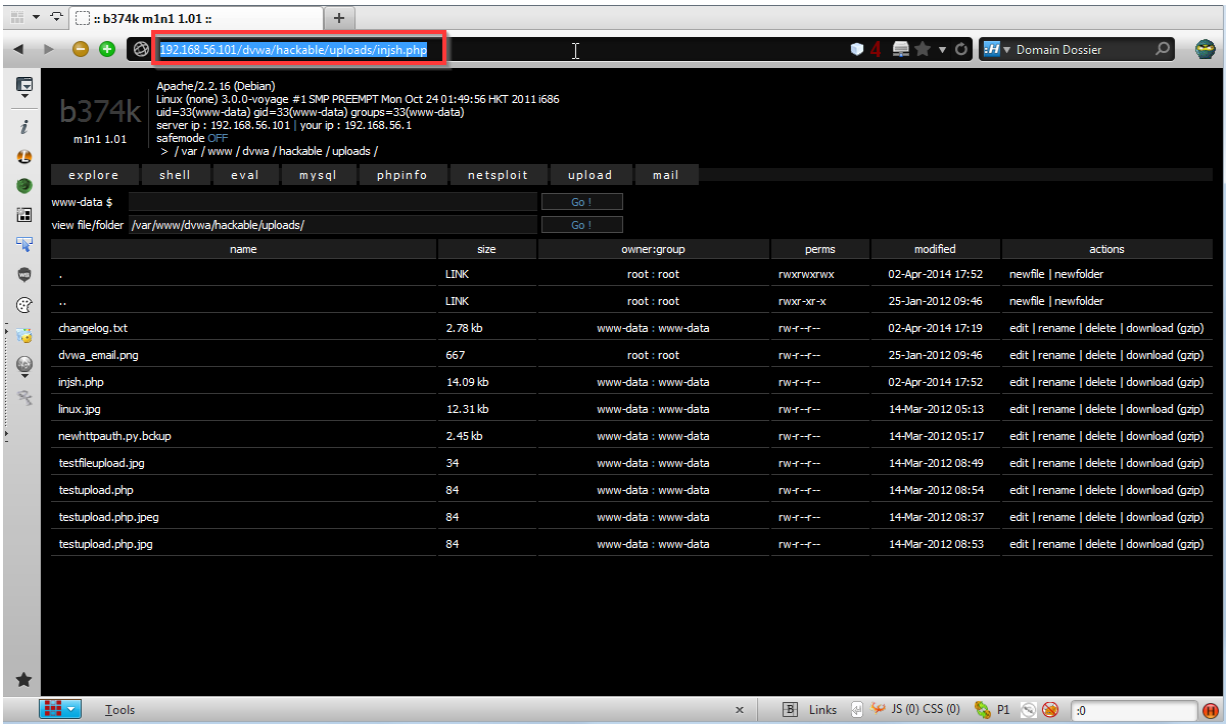

:: b374k m1n1 1.01 ::
192.168.56.101/dvwa/hackable/uploads/injsh.php
Domain Dossier
b374k
m1n1 1.01
Apache/2.2.16 (Debian)
Linux (none) 3.0.0-voyage #1 SMP PREEMPT Mon Oct 24 01:49:56 HKT 2011 i686
uid=33(www-data) gid=33(www-data) groups=33(www-data)
server ip : 192.168.56.101 | your ip : 192.168.56.1
safemode OFF
> / var / www / dvwa / hackable / uploads /
explore shell eval mysql phpinfo netsploit upload mail
www-data $
Go !
view file/folder /var/www/dvwa/hackable/uploads/
Go !
name size owner:group perms modified actions
. LINK root : root rwxrwxrwx 02-Apr-2014 17:52 newfile | newfolder
.. LINK root : root rwxr-xr-x 25-Jan-2012 09:46 newfile | newfolder
changelog.txt 2.78 kb www-data : www-data rw-r--r-- 02-Apr-2014 17:19 edit | rename | delete | download (gzip)
dvwa_email.png 667 root : root rw-r--r-- 25-Jan-2012 09:46 edit | rename | delete | download (gzip)
injsh.php 14.09 kb www-data : www-data rw-r--r-- 02-Apr-2014 17:52 edit | rename | delete | download (gzip)
linux.jpg 12.31 kb www-data : www-data rw-r--r-- 14-Mar-2012 05:13 edit | rename | delete | download (gzip)
newhttpauth.py.bckup 2.45 kb www-data : www-data rw-r--r-- 14-Mar-2012 05:17 edit | rename | delete | download (gzip)
testfileupload.jpg 34 www-data : www-data rw-r--r-- 14-Mar-2012 08:49 edit | rename | delete | download (gzip)
testupload.php 84 www-data : www-data rw-r--r-- 14-Mar-2012 08:54 edit | rename | delete | download (gzip)
testupload.php.jpeg 84 www-data : www-data rw-r--r-- 14-Mar-2012 08:37 edit | rename | delete | download (gzip)
testupload.php.jpg 84 www-data : www-data rw-r--r-- 14-Mar-2012 08:53 edit | rename | delete | download (gzip)
Tools
Links
JS (0) CSS (0)
P1

Figure 100: B37AK webshell running on server

Now we have a backdoor webshell uploaded to the server, using this we can do almost all kind of things depending on which shell we are using. most of the shells has features like port scanning, database hack, cpanel cracking, file upload/download, backconnect, fake mailer and much more to compromise the whole server. Accessing the passwd file of the remote server via webshell.

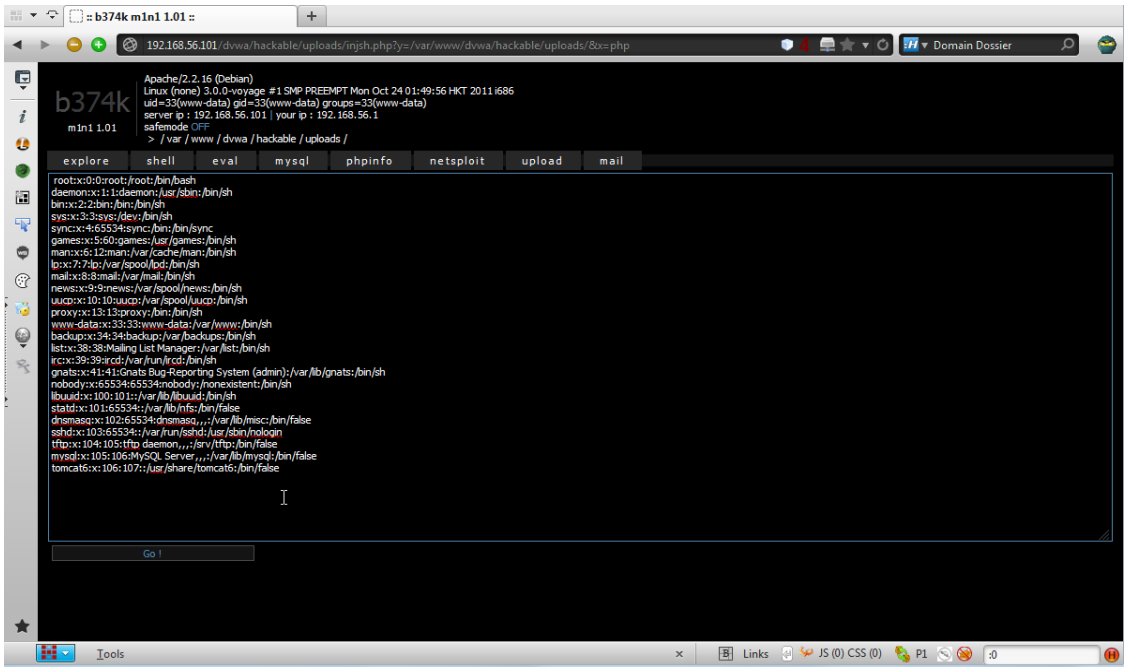


Figure 101: Accessing remote file system

5.3 Request Manipulation

5.3.1 Inspecting Request

Inspecting web requests and responses can give lot of logical and functional information about target webapp. some of the common information can be found from this is,

- HTTP methods used
- HTTP status codes on requests and its responses
- POST form fields
- Cookie information
- Host information
- Content-type
- Special headers from server side framework

let we inspect web requests and responses when we load DVWA and login into it.

open DVWA in HconSTF

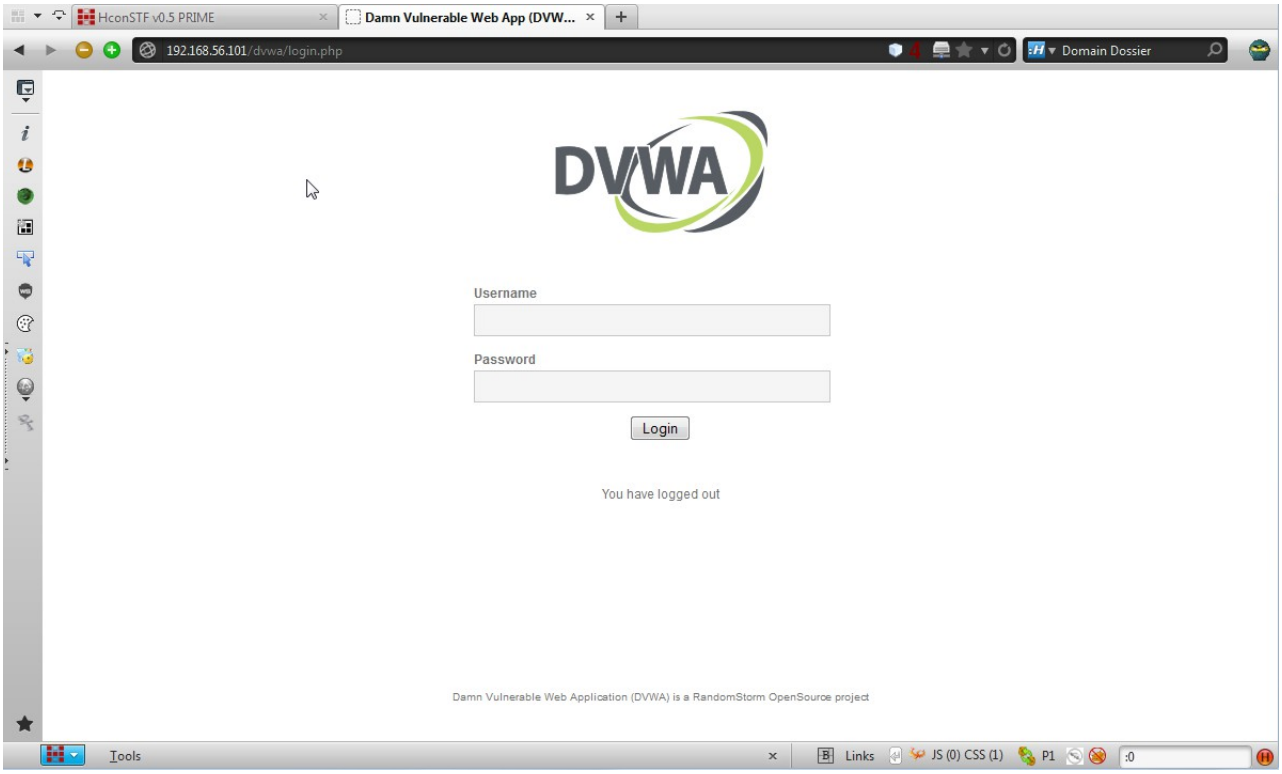


Figure 102: DVWA opened in HconSTF

Now start a tool from Hmenu → Recon/Mapping → HttpFox → Open In own Window

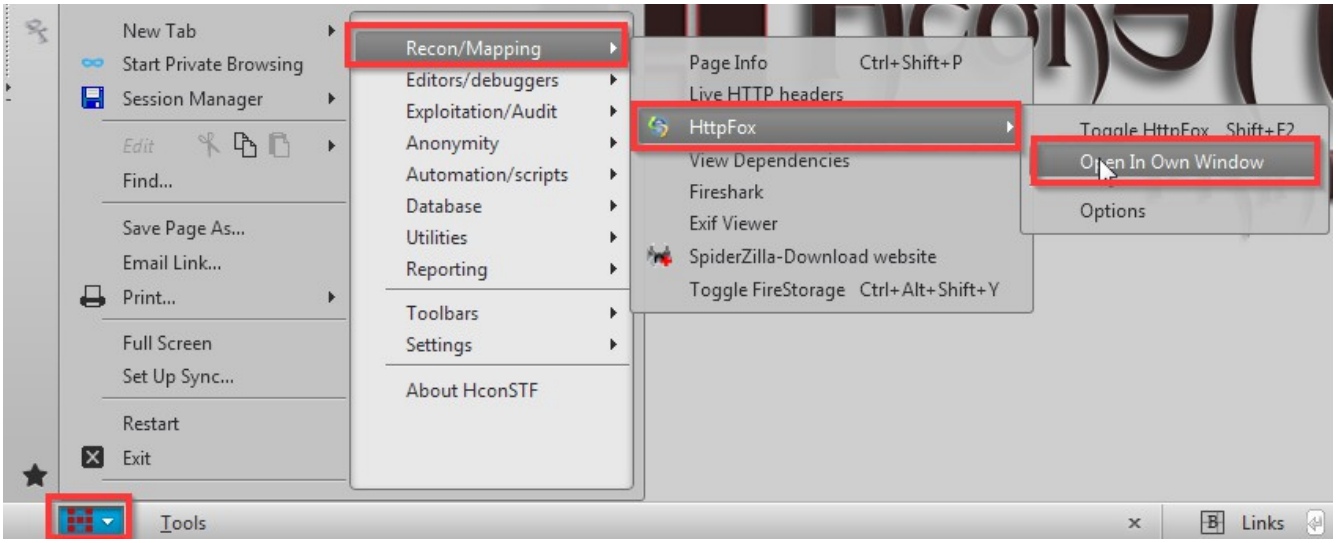


Figure 103: HTTPfox in HconSTF

This will open up tool for inspecting web requests in a new window, now click on 'Start' and refresh the DVWA page.

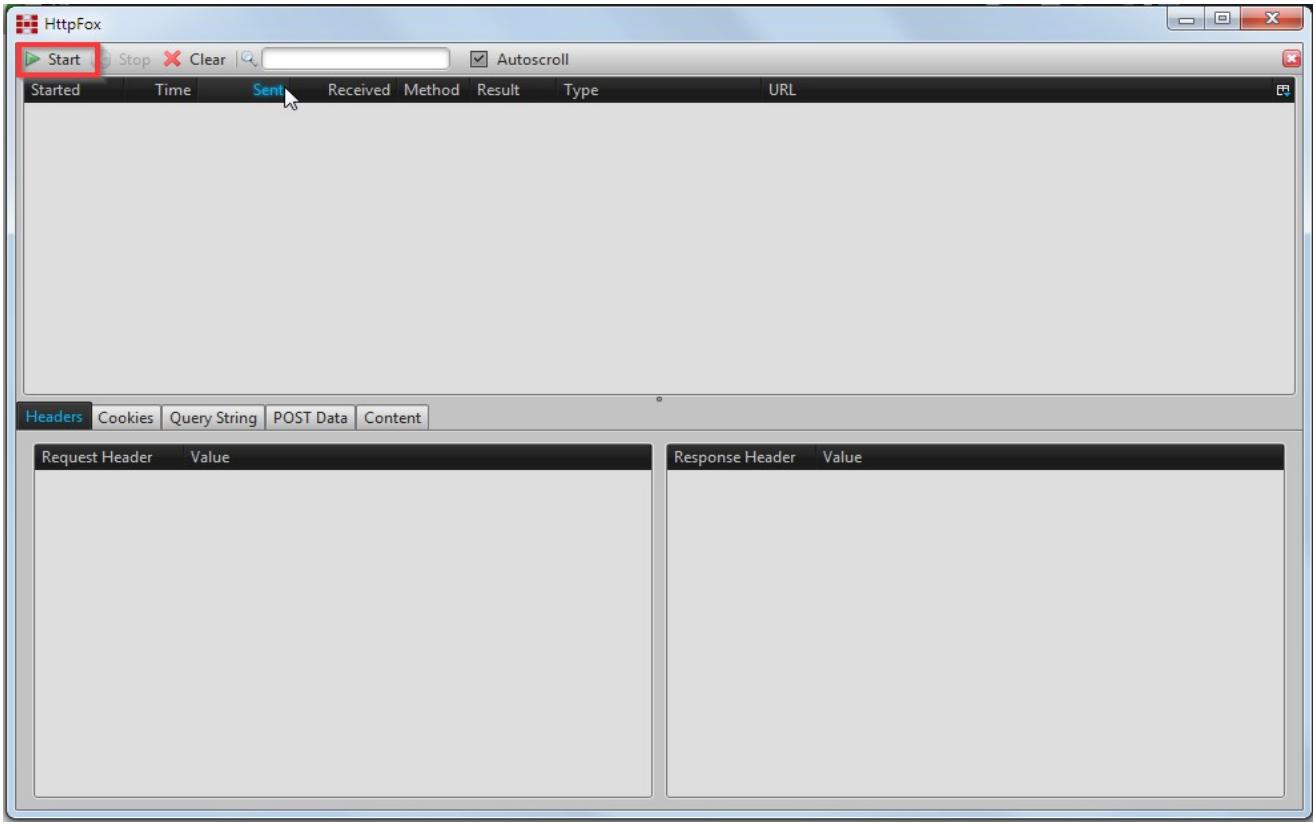


Figure 104: Starting logging http traffic

Now enter credentials admin:password and login to DVWA. let us inspect the web request in Httpfox inspector window.

We see that as we logged in, the webapp redirected from index.php to login.php and sent form field data using POST http method with http status code of 302 which is for redirect request, note that webapp uses HTTP version 1.1

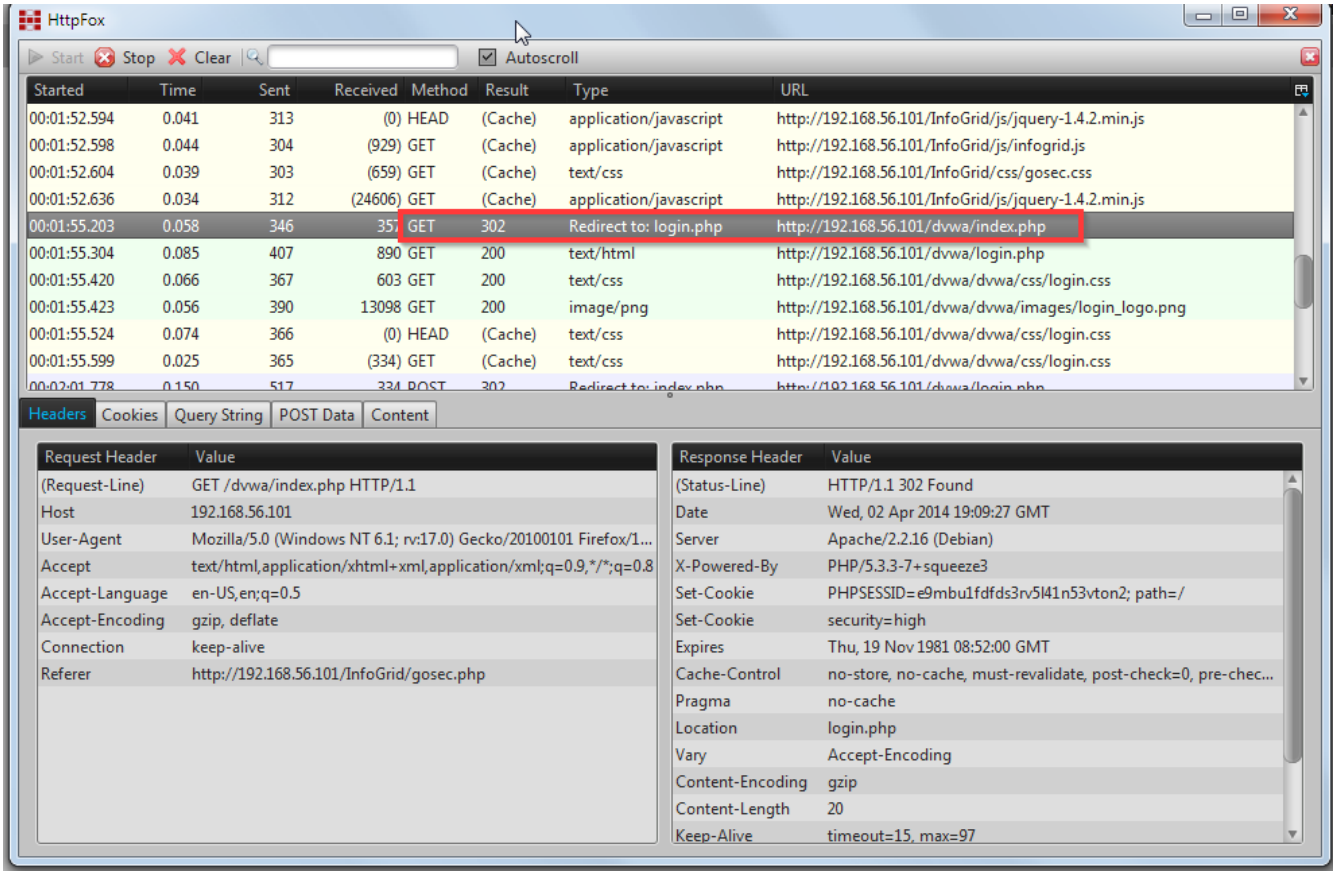

HttpFox
Start
Stop
Clear
Autoscroll
Started Time Sent Received Method Result Type URL
00:01:52.594 0.041 313 (0) HEAD (Cache) application/javascript http://192.168.56.101/InfoGrid/js/jquery-1.4.2.min.js
00:01:52.598 0.044 304 (929) GET (Cache) application/javascript http://192.168.56.101/InfoGrid/js/infogrid.js
00:01:52.604 0.039 303 (659) GET (Cache) text/css http://192.168.56.101/InfoGrid/css/gosec.css
00:01:52.636 0.034 312 (24606) GET (Cache) application/javascript http://192.168.56.101/InfoGrid/js/jquery-1.4.2.min.js
00:01:55.203 0.058 346 357 GET 302 Redirect to: login.php http://192.168.56.101/dvwa/index.php
00:01:55.304 0.085 407 890 GET 200 text/html http://192.168.56.101/dvwa/login.php
00:01:55.420 0.066 367 603 GET 200 text/css http://192.168.56.101/dvwa/dvwa/css/login.css
00:01:55.423 0.056 390 13098 GET 200 image/png http://192.168.56.101/dvwa/dvwa/images/login_logo.png
00:01:55.524 0.074 366 (0) HEAD (Cache) text/css http://192.168.56.101/dvwa/dvwa/css/login.css
00:01:55.599 0.025 365 (334) GET (Cache) text/css http://192.168.56.101/dvwa/dvwa/css/login.css
Headers Cookies Query String POST Data Content
Request Header Value
(Request-Line) GET /dvwa/index.php HTTP/1.1
Host 192.168.56.101
User-Agent Mozilla/5.0 (Windows NT 6.1; rv:17.0) Gecko/20100101 Firefox/1...
Accept text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language en-US,en;q=0.5
Accept-Encoding gzip, deflate
Connection keep-alive
Referer http://192.168.56.101/InfoGrid/gosec.php
Response Header Value
(Status-Line) HTTP/1.1 302 Found
Date Wed, 02 Apr 2014 19:09:27 GMT
Server Apache/2.2.16 (Debian)
X-Powered-By PHP/5.3.3-7+squeeze3
Set-Cookie PHPSESSID=e9mbu1fdfds3rv5l41n53vton2; path=/
Set-Cookie security=high
Expires Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control no-store, no-cache, must-revalidate, post-check=0, pre-chec...
Pragma no-cache
Location login.php
Vary Accept-Encoding
Content-Encoding gzip
Content-Length 20
Keep-Alive timeout=15, max=97

Figure 105: 302 Redirect request and its contents

From the same window we can see the server responded with lots of server side technological information with version numbers.

After processing credentials the page redirected to index.php and we can see the sent form fields

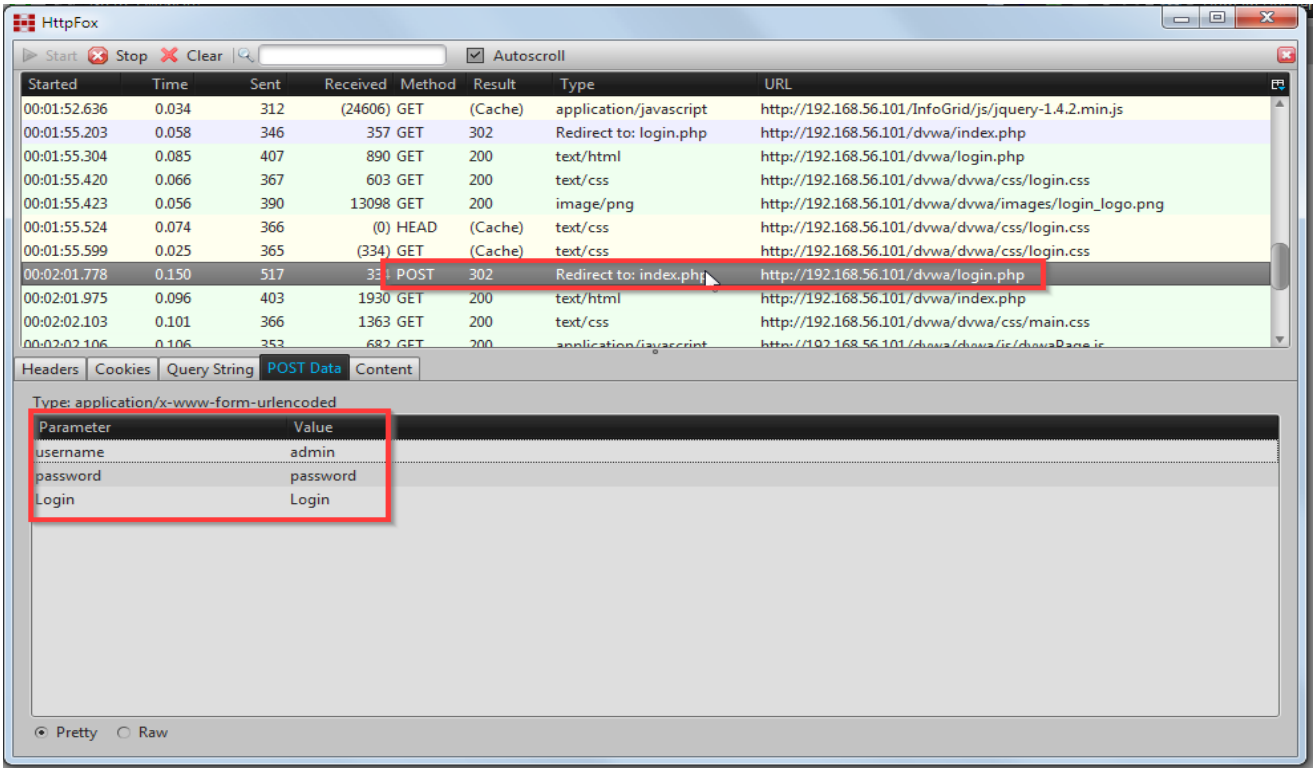

HttpFox
Start
Stop
Clear
Autoscroll
Started Time Sent Received Method Result Type URL
00:01:52.636 0.034 312 (24606) GET (Cache) application/javascript http://192.168.56.101/InfoGrid/js/jquery-1.4.2.min.js
00:01:55.203 0.058 346 357 GET 302 Redirect to: login.php http://192.168.56.101/dvwa/index.php
00:01:55.304 0.085 407 890 GET 200 text/html http://192.168.56.101/dvwa/login.php
00:01:55.420 0.066 367 603 GET 200 text/css http://192.168.56.101/dvwa/dvwa/css/login.css
00:01:55.423 0.056 390 13098 GET 200 image/png http://192.168.56.101/dvwa/dvwa/images/login_logo.png
00:01:55.524 0.074 366 (0) HEAD (Cache) text/css http://192.168.56.101/dvwa/dvwa/css/login.css
00:01:55.599 0.025 365 (334) GET (Cache) text/css http://192.168.56.101/dvwa/dvwa/css/login.css
00:02:01.778 0.150 517 POST 302 Redirect to: index.php http://192.168.56.101/dvwa/login.php
00:02:01.975 0.096 403 1930 GET 200 text/html http://192.168.56.101/dvwa/index.php
00:02:02.103 0.101 366 1363 GET 200 text/css http://192.168.56.101/dvwa/dvwa/css/main.css
Headers Cookies Query String POST Data Content
Type: application/x-www-form-urlencoded
Parameter Value
username admin
password password
Login Login
Pretty Raw

Figure 106: Sent data and form fields in POST

We can also see other content types like js, css, html, img, png etc. which is being transferred in http traffic and we can also see raw and rendered data for the same.

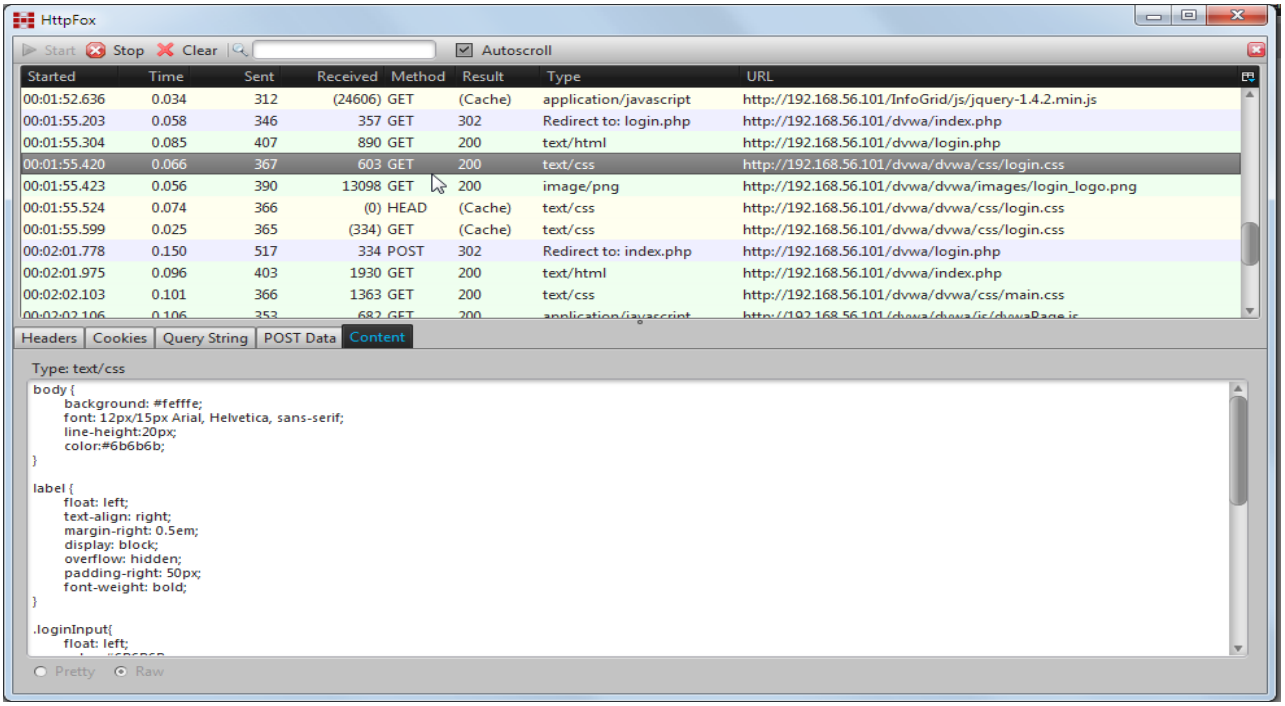


Figure 107: Inspecting raw data from http traffic

This is very useful method of getting information out and learning the application logic and functioning before testing it.

5.3.2 Intercepting Request

Intercepting any web request is very useful when,

- Trying to bypass client side security controls
- Injecting attack payloads
- Parameter tampering
- Adding more content into request
- Manipulating hidden fields

by all of the above making webapp to behave in uncertain way.

We already seen how to intercept requests in 'File upload' section of testing for vulnerabilities chapter 5.2.3 in that we intercepted the web requests and modified the POST field data, which was not possible by direct uploading using the file upload form.

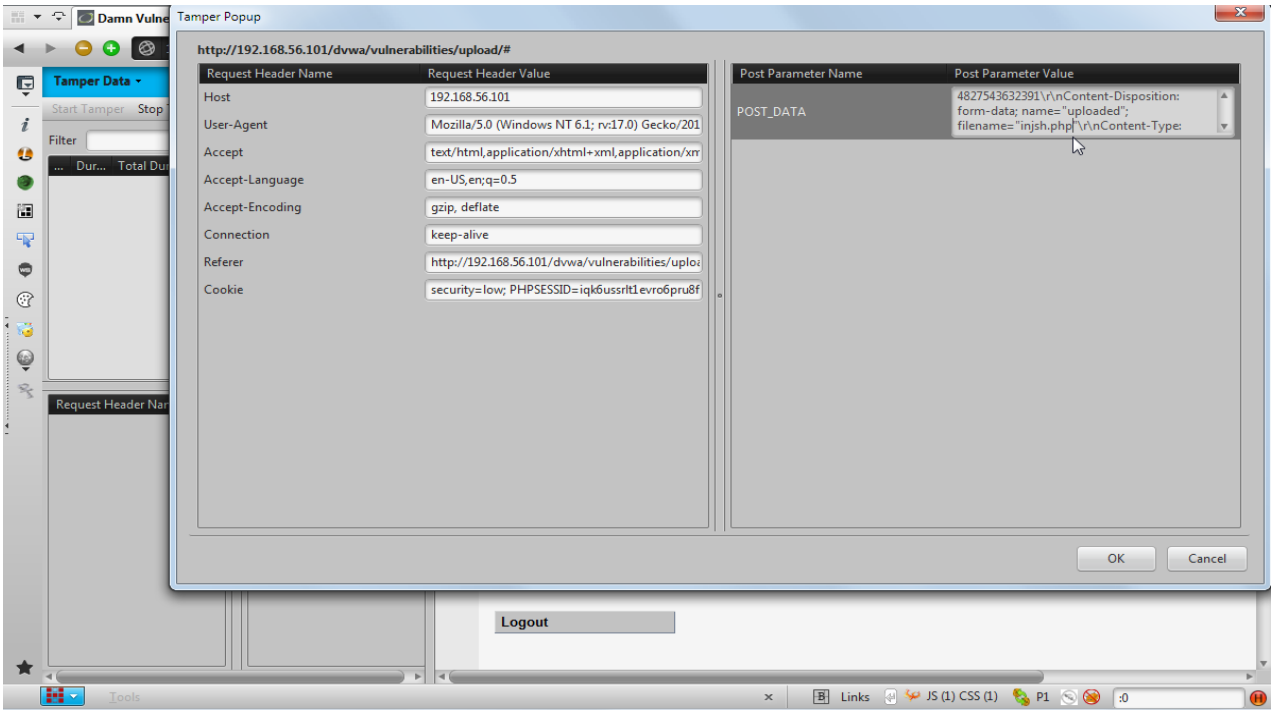


Figure 108: Manipulating http request data

Other then this we can change request header information and also inject new form fields or inject attack payloads such as XSS, SQLi into the post data.

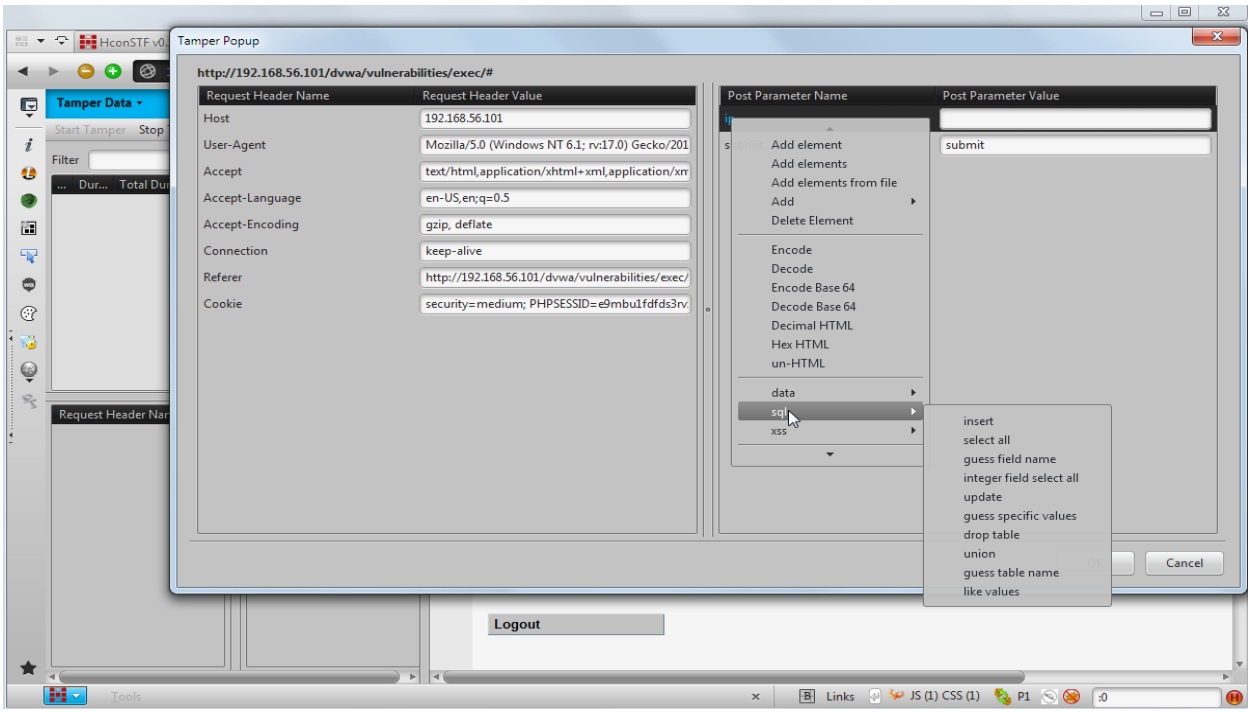


Figure 109: Injecting attack strings and more form elements

Intercepting and sending more crafted data to webapp is very powerful in whole webapp testing process and is only limited to our imagination of how we use the intercepting request feature.

5.3.3 Replaying Request

Request replaying is basically running the same request but with few parameter changed which can be,

- Protocol
- Host
- Port
- Path
- Reference
- Credentials
- Request header information
- GET and POST fields

This can be really useful for testing whether access controls are implemented properly or not by changing individual parameters for the same request to the webapp, depending on the content and in which context we change single parameter the webapp will going to behave differently and can lead to many different kind of attacks.

Let us see replaying web request with HconSTF, open All sidebar panels button → Tamper data

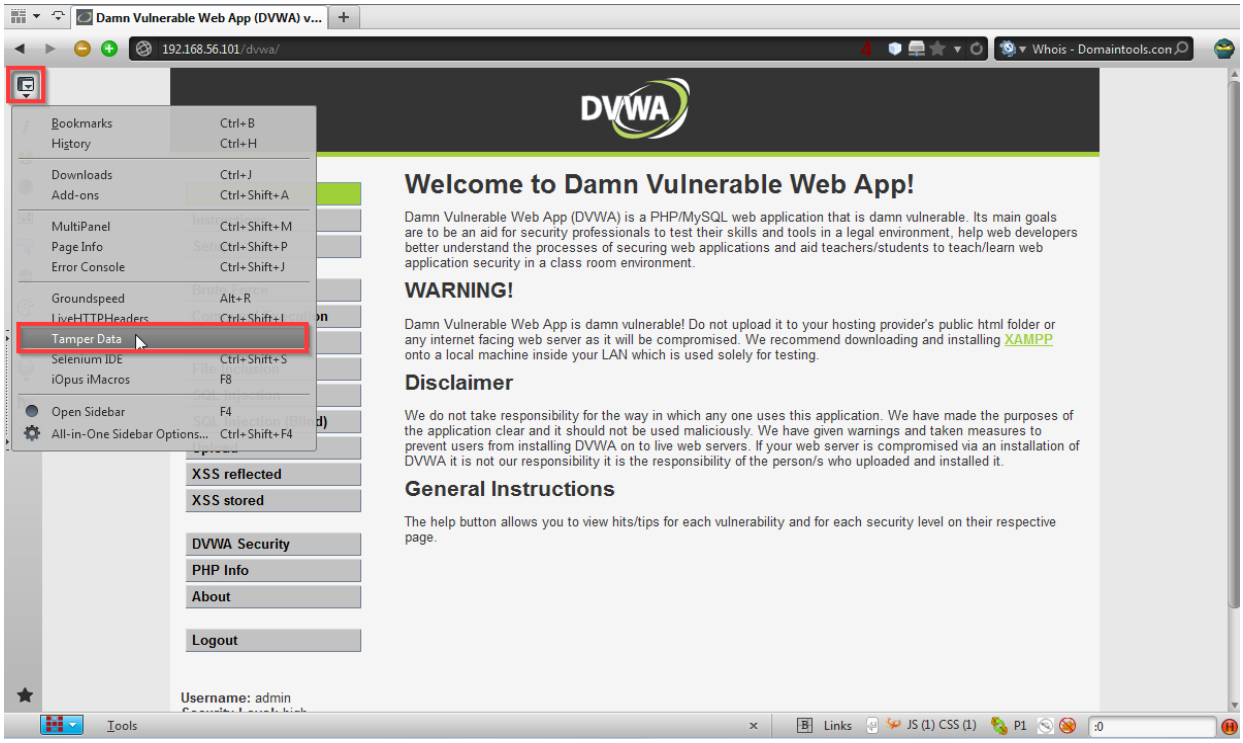

Damn Vulnerable Web App (DVWA) v...
192.168.56.101/dvwa/
Whois - Domaintools.com
Bookmarks Ctrl+B
History Ctrl+H
Downloads Ctrl+J
Add-ons Ctrl+Shift+A
MultiPanel Ctrl+Shift+M
Page Info Ctrl+Shift+P
Error Console Ctrl+Shift+J
Groundspeed Alt+R
Tamper Data
Selenium IDE Ctrl+Shift+S
iOpus iMacros F8
Open Sidebar F4
All-in-One Sidebar Options... Ctrl+Shift+F4
DVWA
Welcome to Damn Vulnerable Web App!
Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.
WARNING!
Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.
Disclaimer
We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
General Instructions
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Username: admin
Tools
Links

Figure 110: Opening Tamper data in sidebar

Now load the file Upload vulnerability page in DVWA and click on 'Upload' button on the page for uploading file.

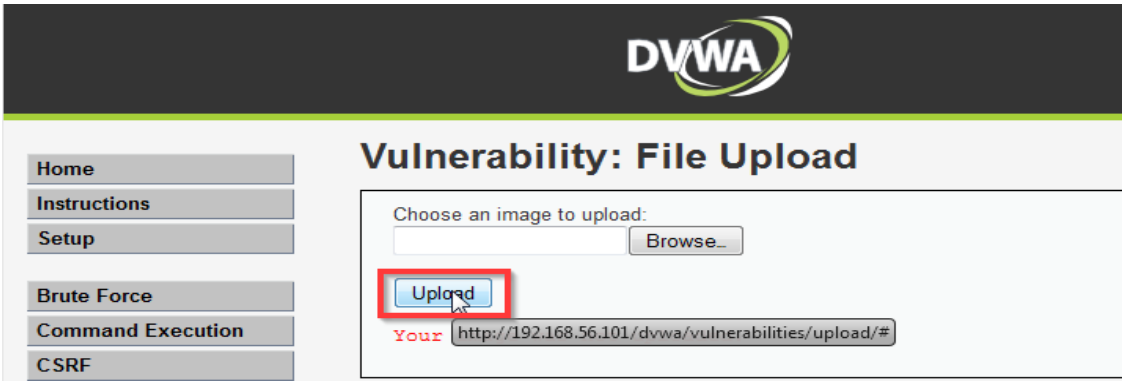


Figure 111: Uploading file in DVWA

As we can see in tamper data sidebar, there is a POST request has been made, right click on that request and select 'Replay in Browser'

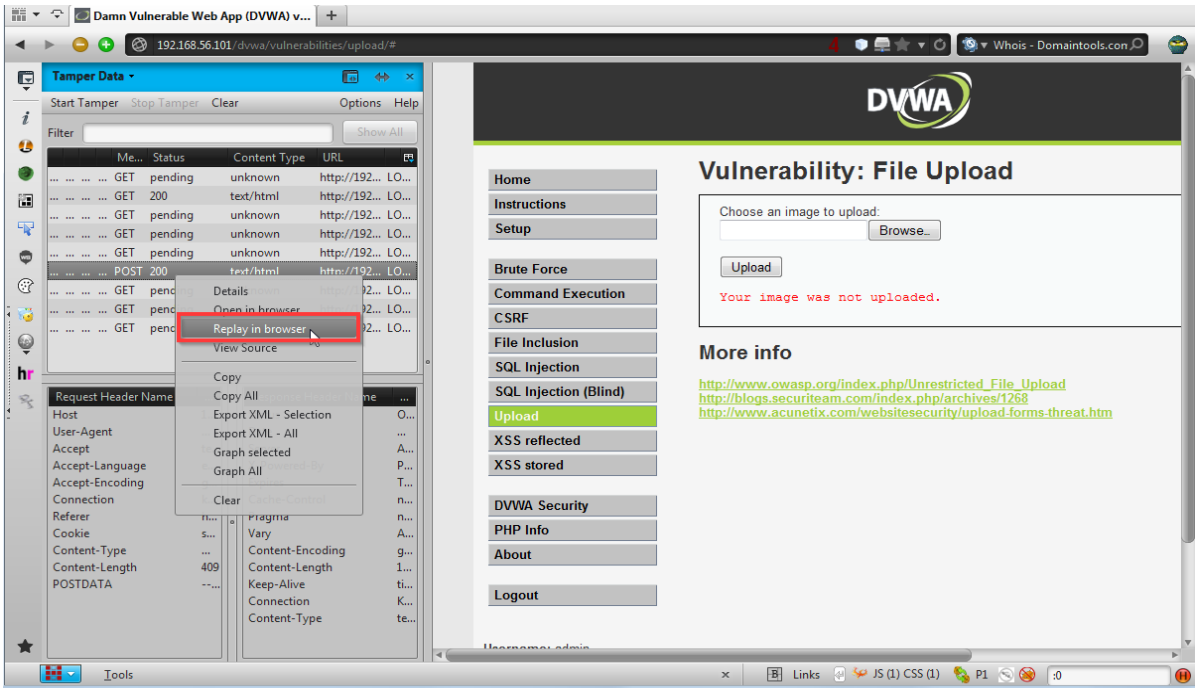


Figure 112: Replay request in browser

In new window, change the parameters or add more elements and click 'OK' to replay the request.

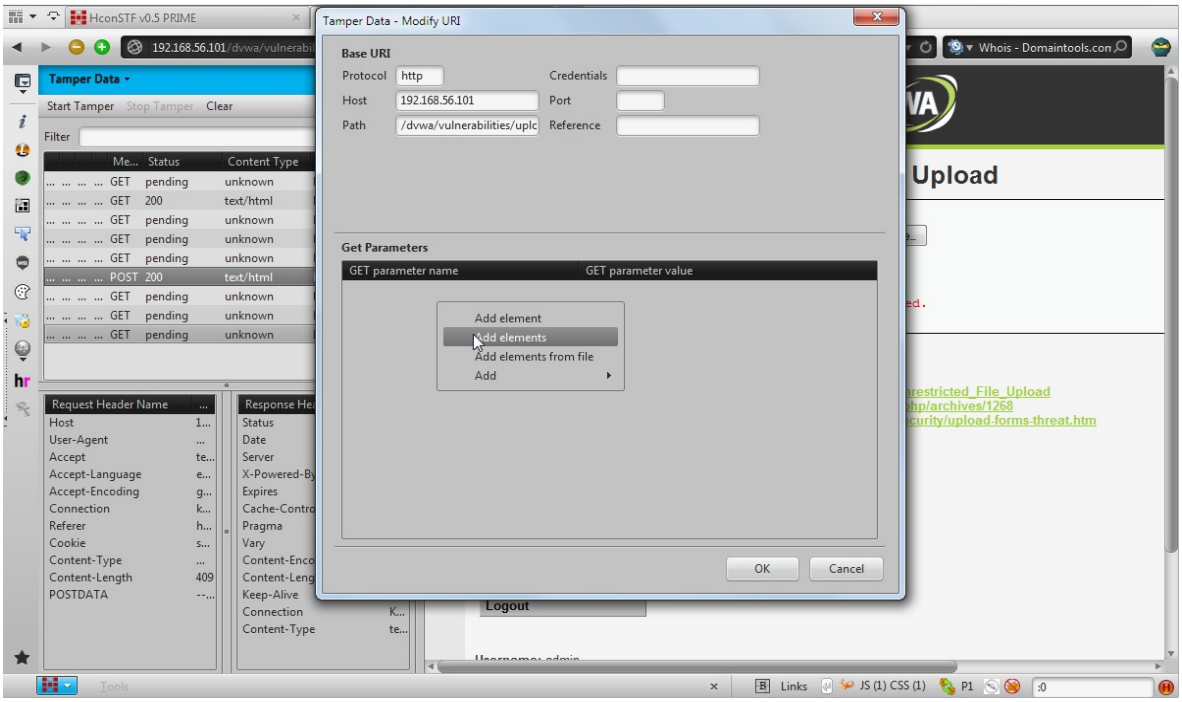


Figure 113: Replay in browser options window

For making more modification in the request and then replaying it, 'Start Tamper' and repeat the process we did above.

Now when we change parameters and click 'OK' for replaying the request it will be intercepted and we can change more fields and add more elements also can inject attack payload.

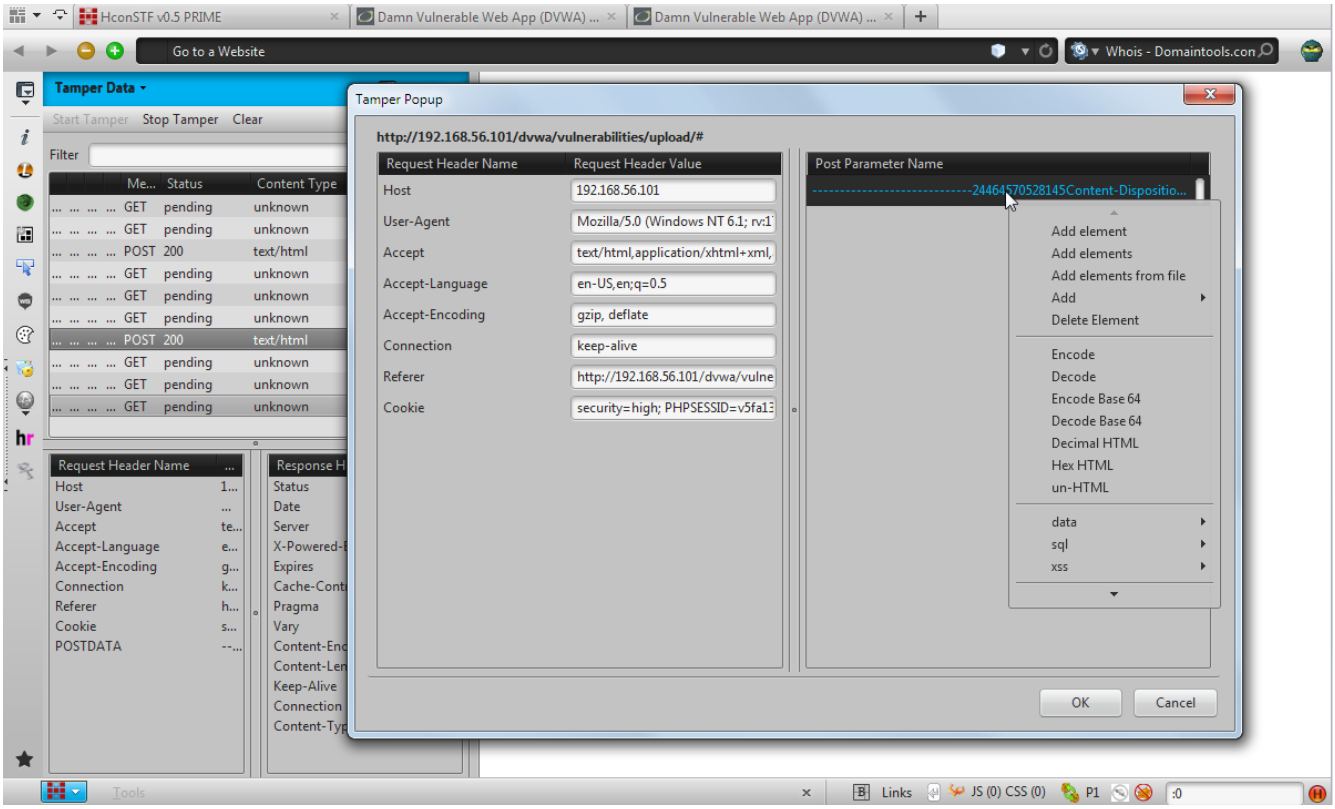


Figure 114: Intercepting then replaying request

5.3.4 Crafting Custom Request

Crafting a custom HTTP request is the best way to manipulate the behavior of the webapp exactly the way we want and this can be useful when we are copying the raw request from other attack and modify it. running it with more transparency with control because we can inspect and work with raw data and not the rendered data.

For crafting custom web requests we can use two-three tools in combination to get work done easily and without any word mistakes. we will be using DVWA and header inspector with http request maker. First start the http header inspector by, clicking on the liveHTTPheaders icon from on the sidebar, and it will open up in new window.

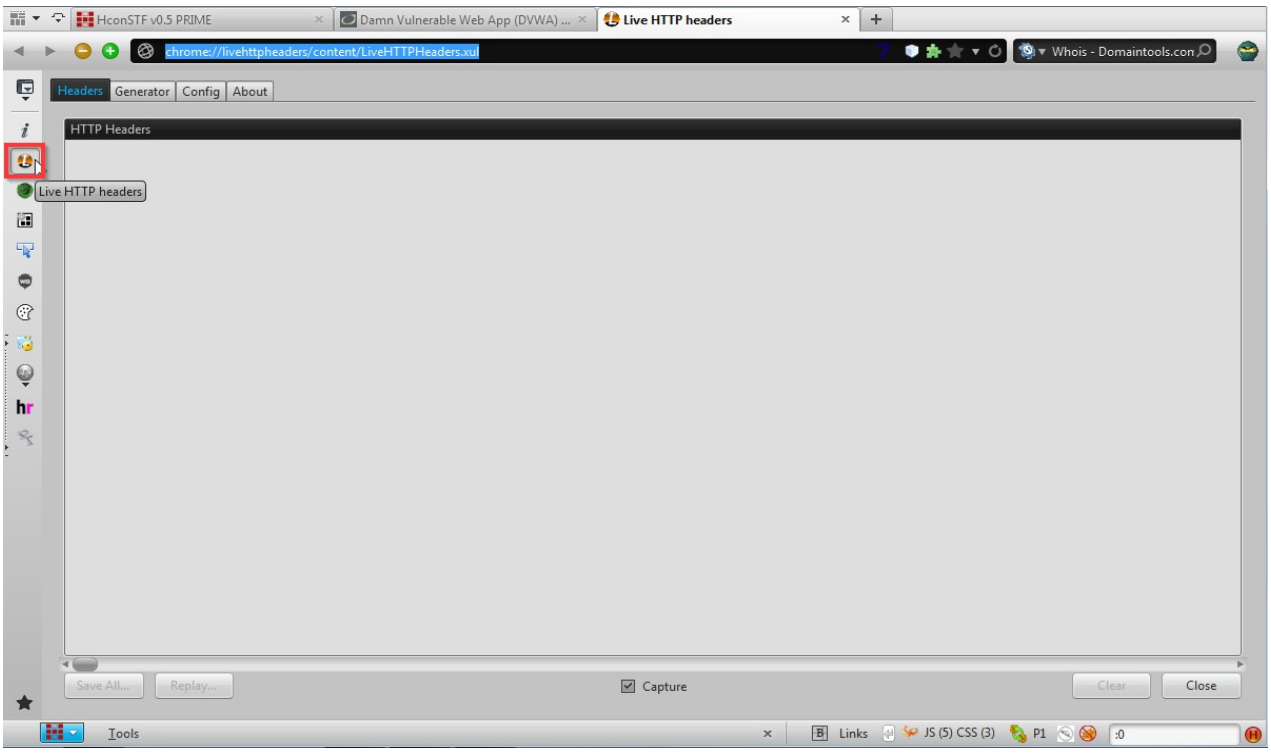


Figure 115: Opening LiveHTTPheaders tool

Now click on the TileTab button at the top left corner in tab bar, it will re arrange the windows side by side for easy inspection.

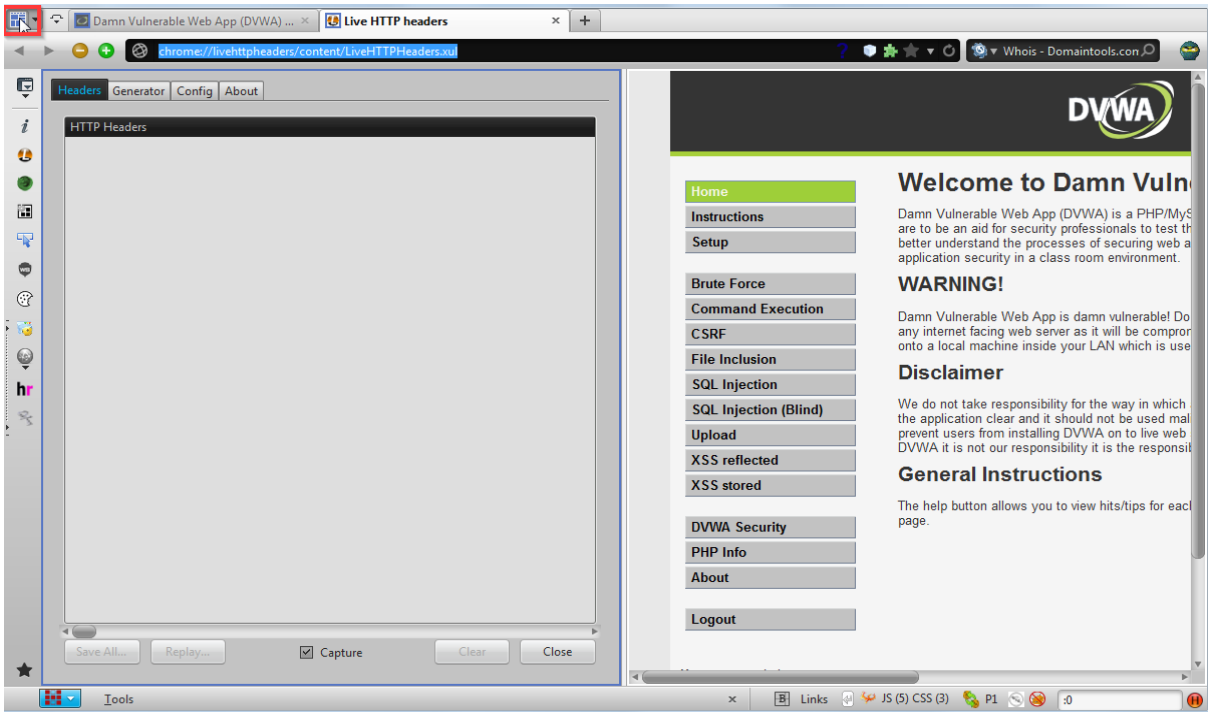


Figure 116: Alining both the windows side by side

Load the CSRF page, and notice the same request has been loaded in Header inspector.

Enter old and new password in form fields and click 'Change' and see the generator tab of header inspector and right click it and copy it. also notice that the password has been changed.

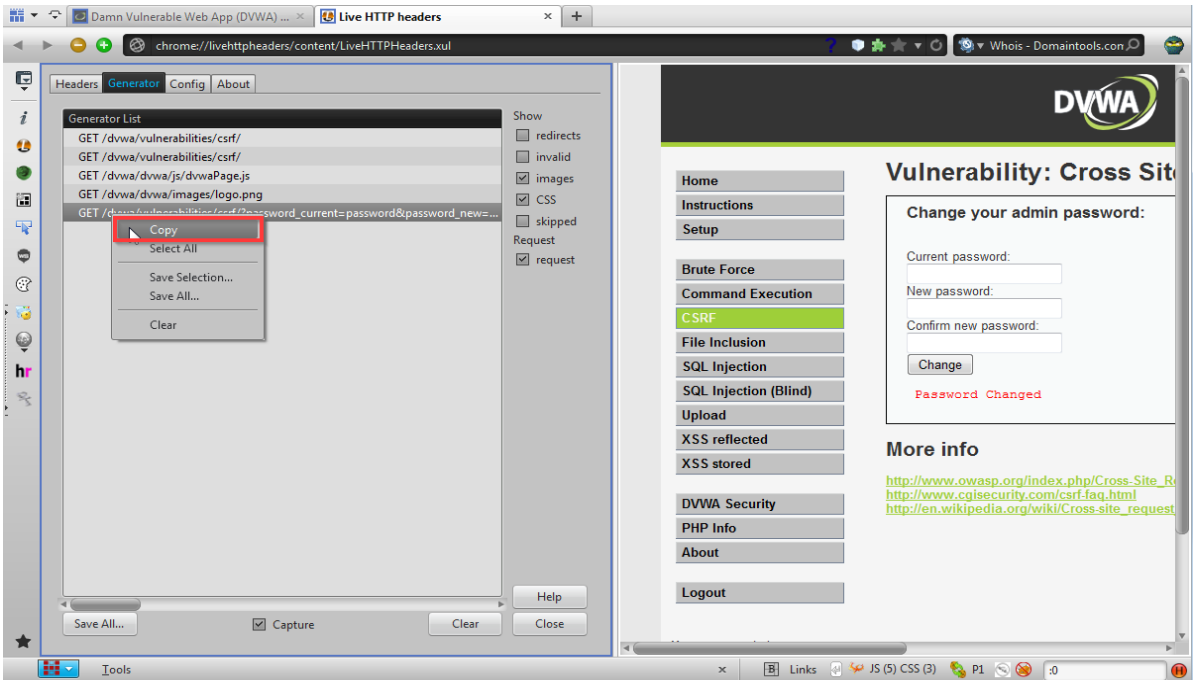


Figure 117: Copy web request from generator tab

Now open Http request maker from Hmenu → Exploitation/Audit → HttpRequester

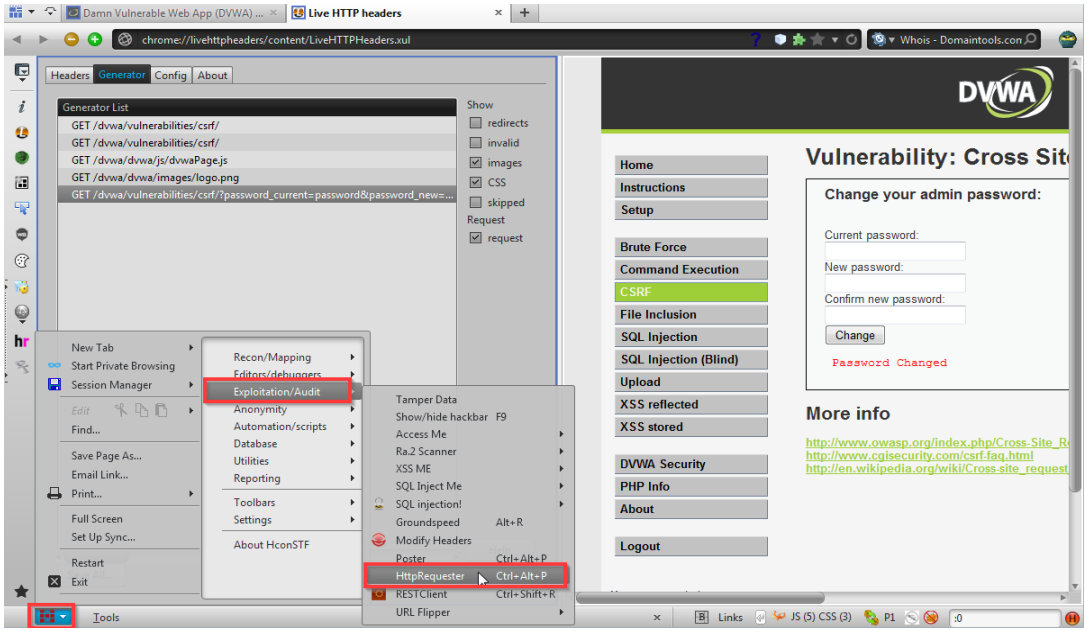


Figure 118: Opening HTTPrequester

Paste that into the URL section of http requester and click on 'submit'

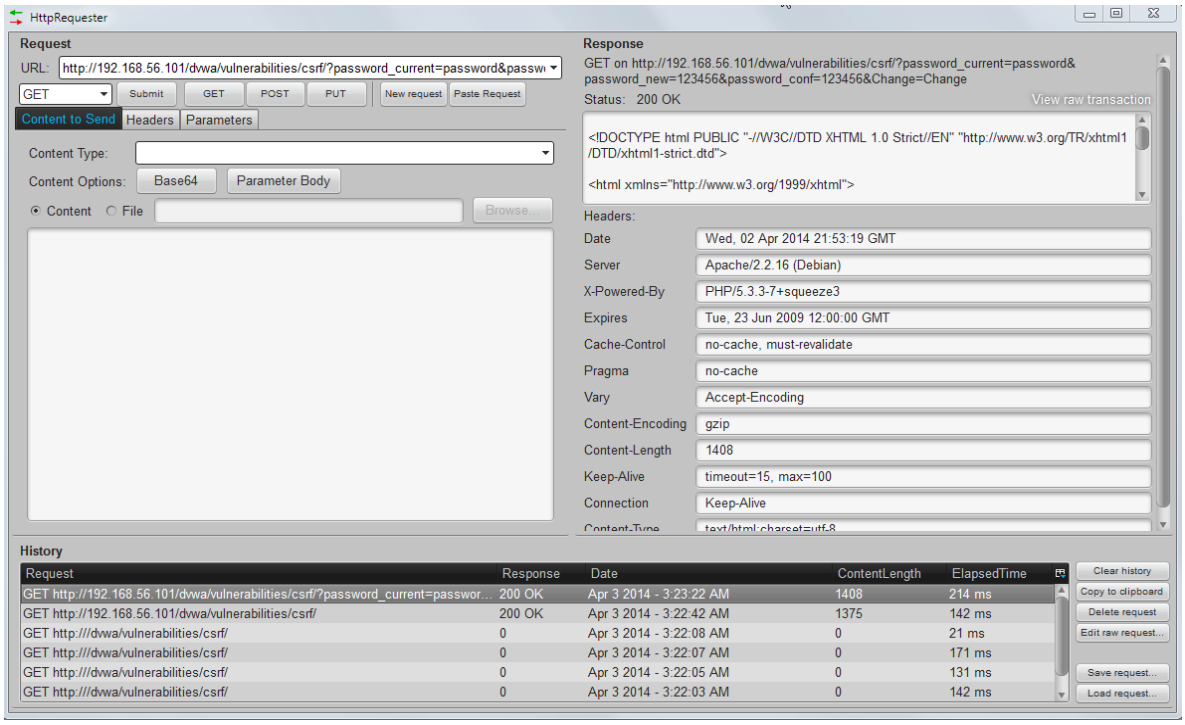


Figure 119: HTTPrequester window with loaded request

As we can see here there is lot of raw data and more parameters that we can modify.

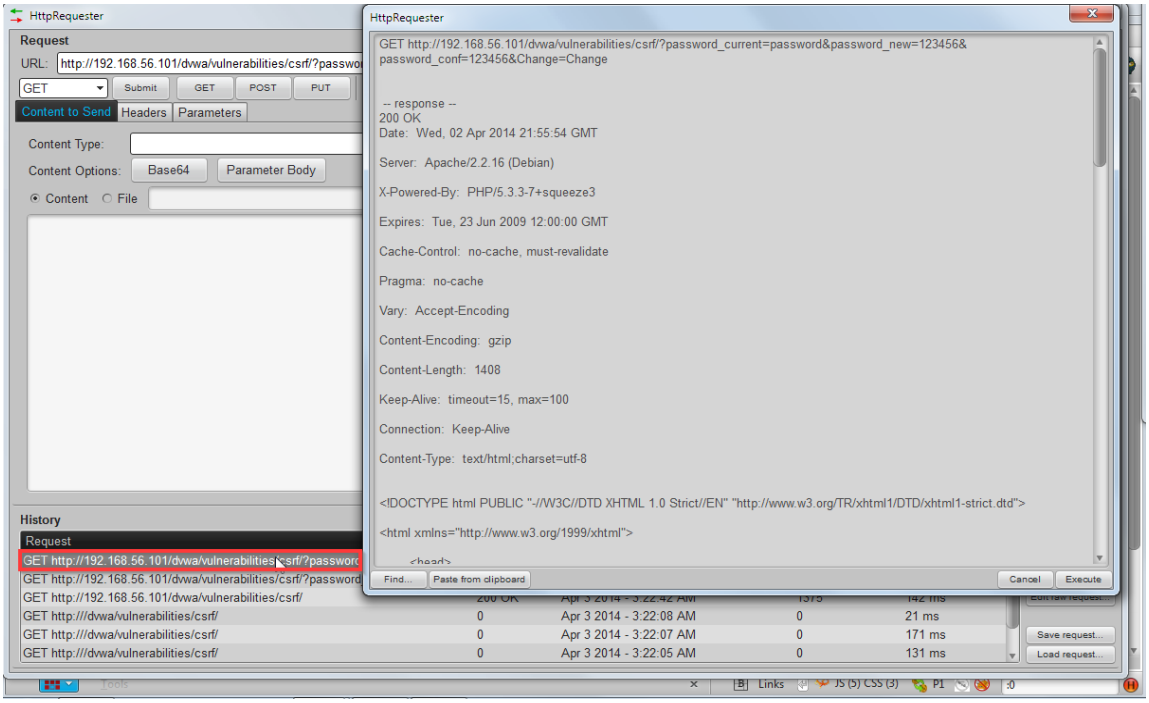


Figure 120: Reading raw data

Now double clicking the last request we did from the history area we can edit the raw request and execute the request. other then this options we can change HTTP methods, add more parameters and header fields, content to send, change content type and much more.

Explore it further with DVWA and practice.

Chapter 6: Cryptography

In this chapter we will look at how to utilize its cryptographic features of hashing / encoding / decoding strings, identifying unknown hashes and even cracking hashes.

6.1 Hashing/Encoding/Decoding

For hashing, encoding and decoding strings in HconSTF,

goto Hmenu → Toolbars → Cryptofox Toolbar

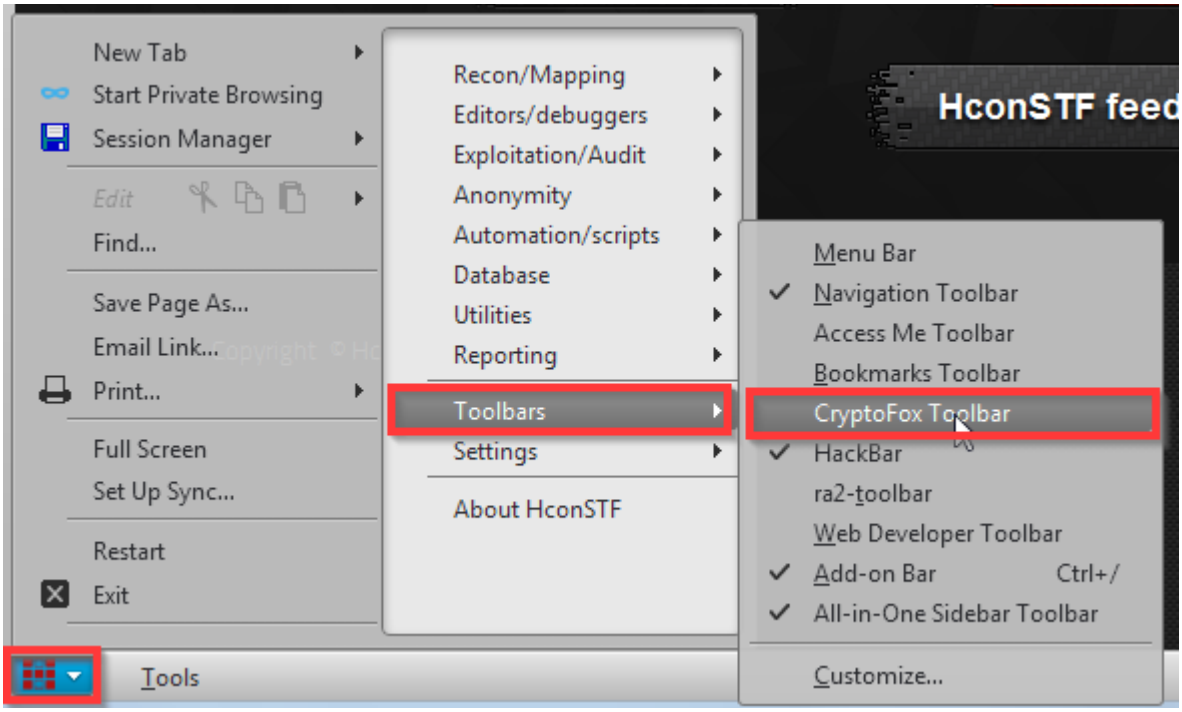


Figure 121: Opening cryptofox toolbar

paste the string in the box and select the algorithm depending on what we want to do with the string and click on 'Encode/Decode'

Figure 122: Encoding a string

it will give resulting value in the same box

Figure 123: Encoded string

We URL encoded the string and we can do the decoding with the same steps with selecting URL decode and click on 'Encode/Decode'

There is one more way of encoding and decoding common algorithms specially in URL and when crafting injection attacks, for that open Hackbar by clicking on green fox icon on the sidebar.

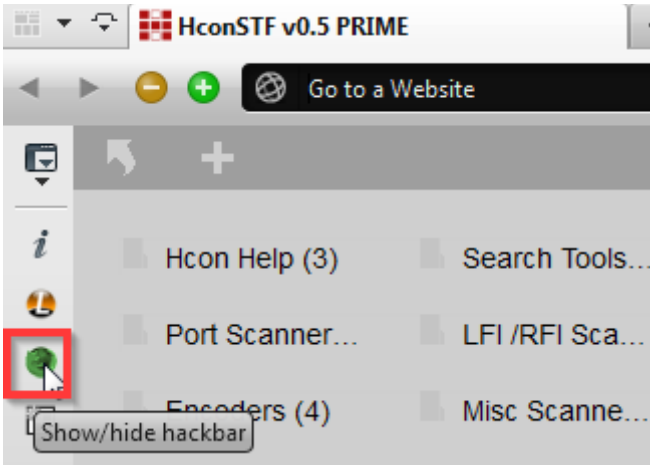


Figure 124: Opening hackbar from sidebar

Else by goto Hmenu → Exploitation/audit → show/hide Hackbar

This will open up hackbar below url bar, as it supports most common URL encode / decode algorithms.

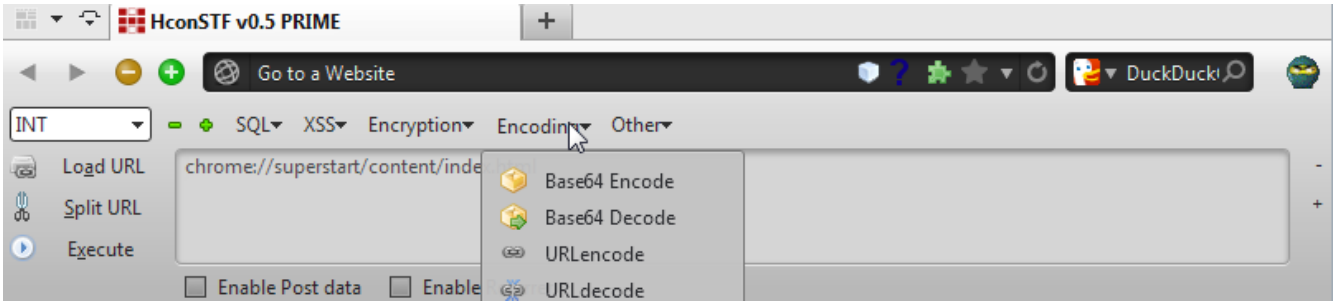


Figure 125: Encoding-decoding options in hackbar

Other then this two mentioned above there are more tools for encoding and decoding in

WebUI → Encoders

There are 4 under this,

- PHP char encoder
- Base64/XML/URL/ECMA script/Character set Encode/Decode
- SQL String Encoder
- Xss String Encoder

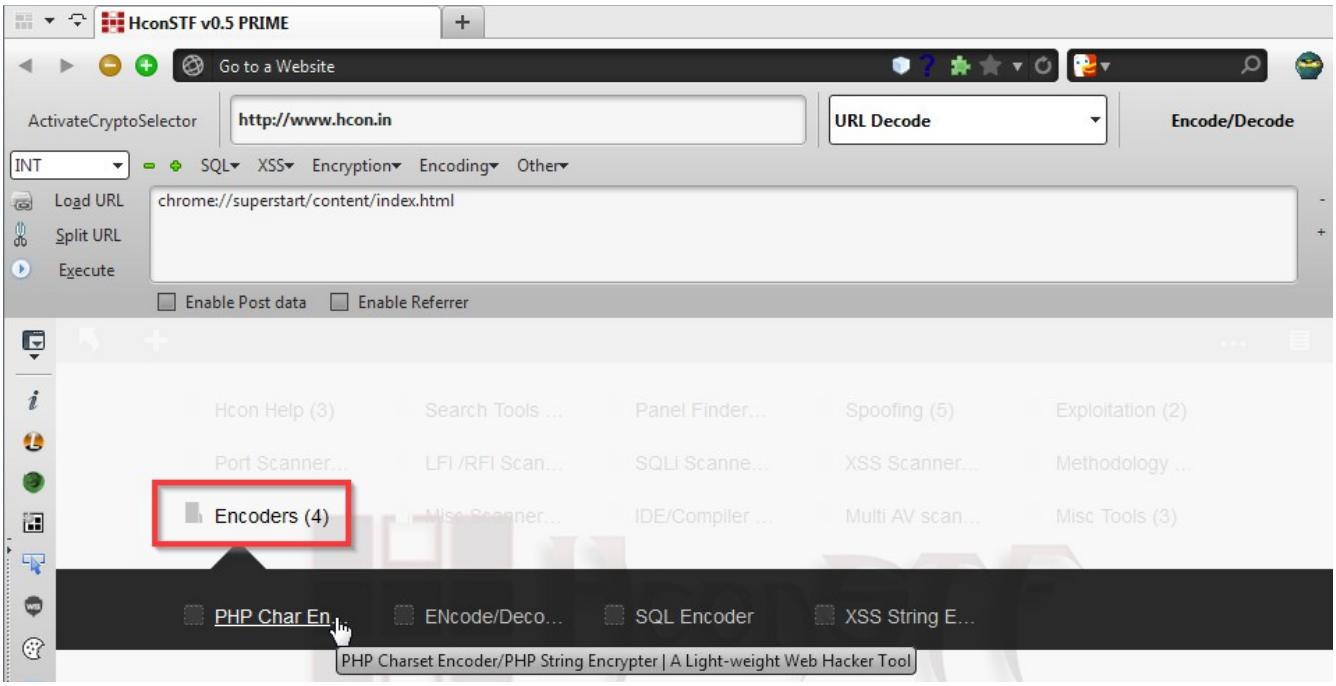


Figure 126: Encoders in WebUI

HconSTF supports wide verity of algorithms for hashing, encoding and decoding:

1. Binary to ASCII/Decimal/Hexadecimal/Octal
2. Octal to Binary/Decimal/Hexadecimal
3. Decimal to Binary/Hexadecimal/Octal
4. Hexadecimal to ASCII/Binary/Decimal/Octal
5. ASCII to Binary/Hexadecimal
6. URL Encode/Decode
7. Base 64 Encode/Decode
8. HTML Entities Encode
9. XML Encode
10. PHP character Encode/Decode
11. SQL String Encode/Decode
12. XSS string Encode/Decode
13. AES 128-bit Encrypt/Decrypt
14. AES 192-bit Encrypt/Decrypt
15. AES 256-bit Encrypt/Decrypt
16. Ceaser Encrypt/Decrypt
17. Morse Code Encrypt/Decrypt
18. MD5 Encrypt
19. DES Encrypt
20. SHA1 Encrypt
21. SHA256 Encrypt
22. Generate CRC32 Checksum
23. Reverse
24. ROT-13
25. XOR Encrypt

6.2 Identifying Unknown Hash

For identifying hash algorithm just select the hash from the webpage and right click → Dork tools → Hash → Identify hash

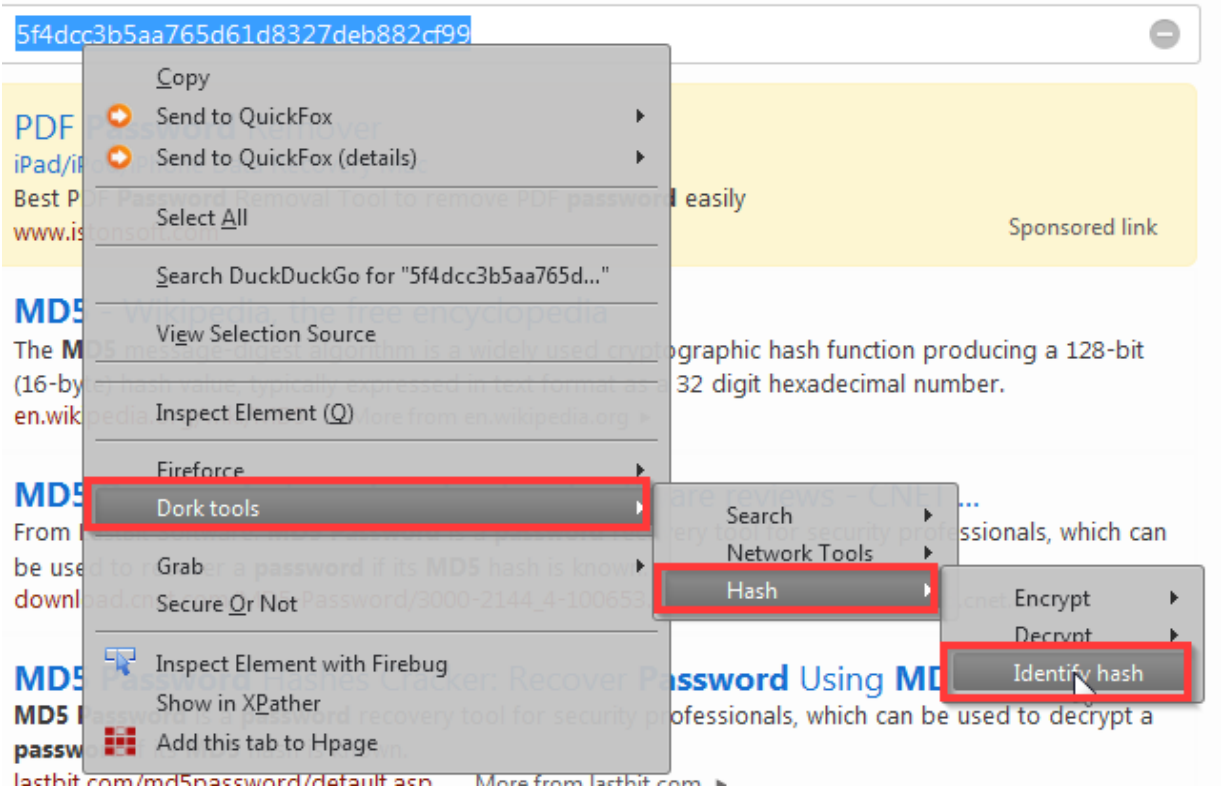


Figure 127: Identifying selected hash on page

we did MD5 'password' by duckduckgo.com and got the same result with other possibilities.

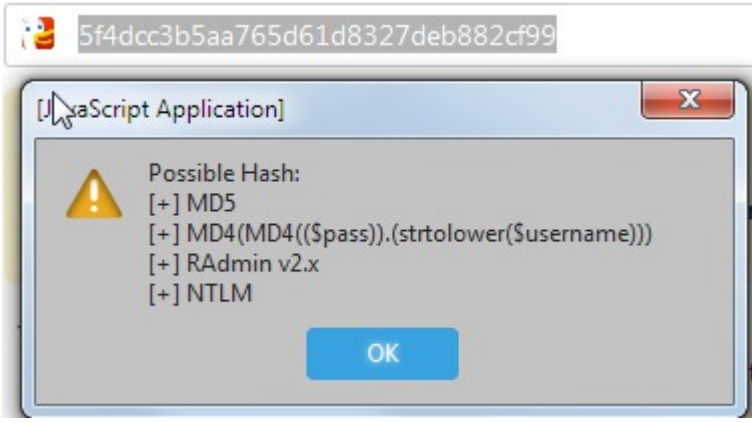


Figure 128: Matching hash detection results

In case that the hash is not on the webpage then we can right click anywhere on the webpage and select Dorktools →Hash → Identify hash and paste the hash we want to identify in the box

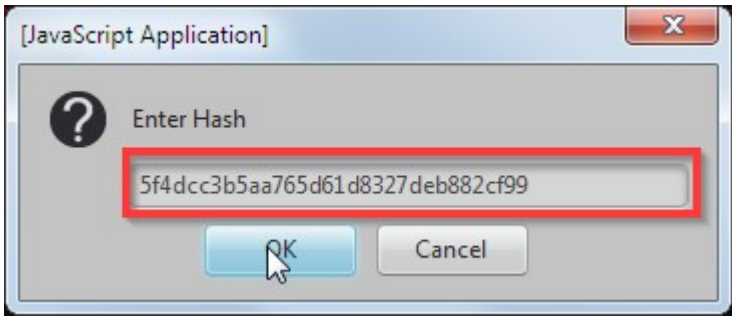


Figure 129: Providing hash value manually

We will going to get the same result as the hash is the same as the previous case.

6.3 Cracking Hashes

We can crack MD5 and SHA1 hashes using HconSTF,

Cracking MD5 Hashes

- Bruteforce it with a wordlist:

For this first we need to open up the tool, goto Hmenu → Toolbars → CryptoFox Toolbar

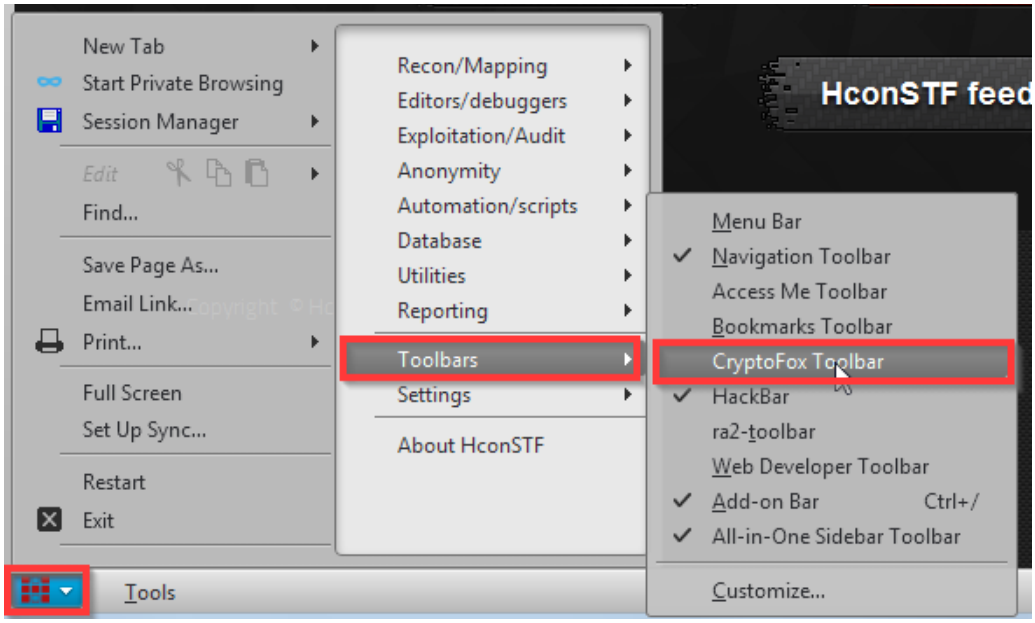


Figure 130: Opening cryptofox toolbar

It will open cryptofox toolbar below the url bar, paste the MD5 hash we want to crack and select 'MD5 Dictionary Attack' and click on 'Encode/Decode'

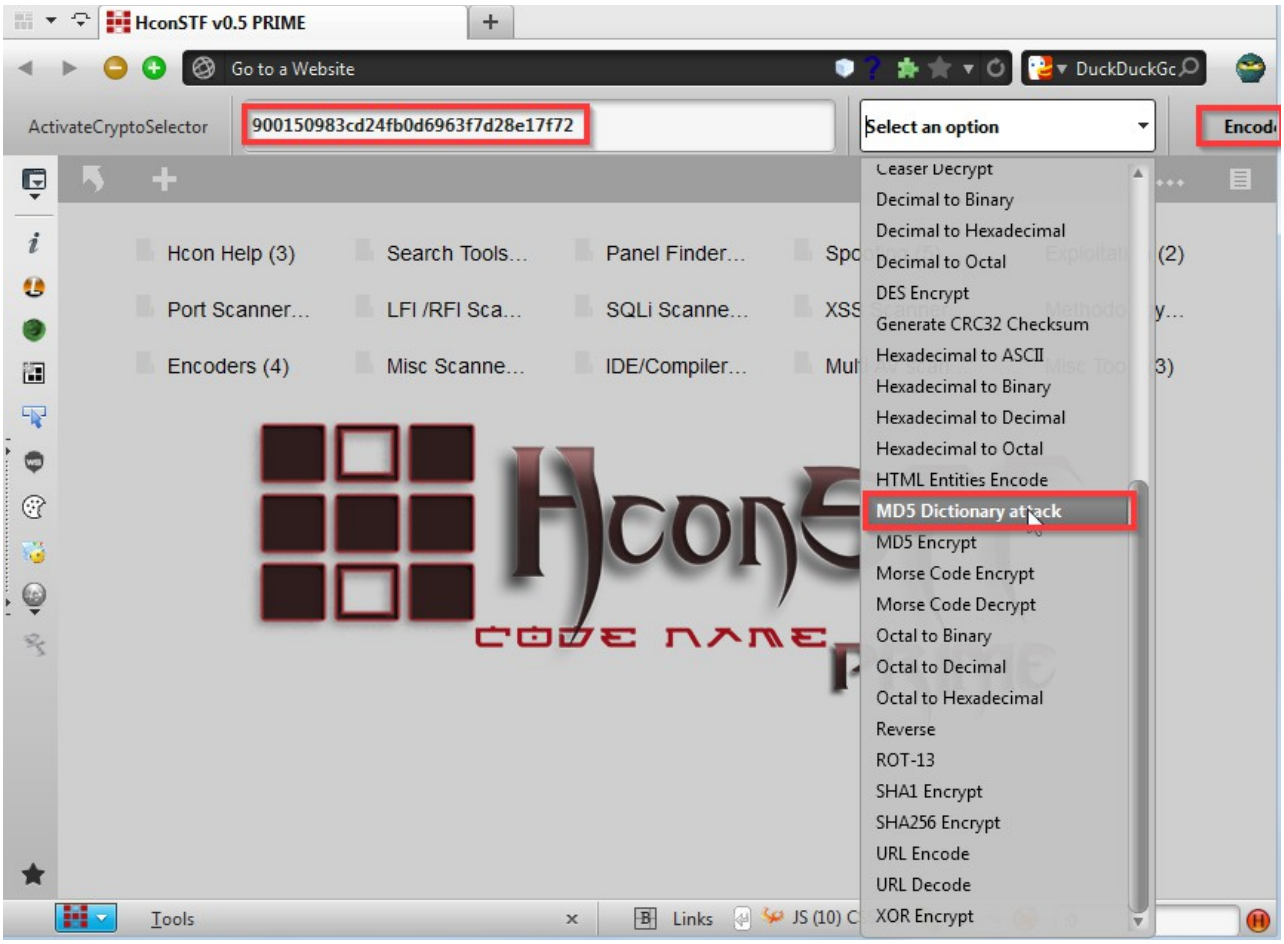


Figure 131: Bruteforcing MD5

It will ask for full path to the wordlist file

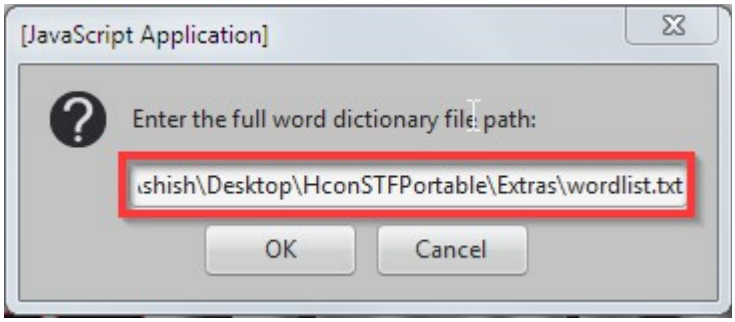


Figure 132: Providing wordlist path

Bruteforcing time will depend on how big the wordlist file is and how quick it matches hash with word.

Figure 133: Decrypted hash value in plain text

Note: *This is a simple dictionary based bruteforcer so the more big or smart our wordlist is the higher the chances of cracking it faster. this method doesn't need internet connectivity.*

- Online hash lookup:

Another way is to use search aggregator and lookup the hash in huge databases of pre-compiled lists. this is applicable for MD5 and SHA1 and few other algorithms. This method is very quick and uses internet connectivity.

paste the hash into the search aggregator or if the hash is on the webpage then just select it and it will be automatically pasted into search aggregator.

select Hash cracker → MD5 or SHA1 try the first three one by one else select each MD5 SET one by one doing 'Open in all tabs'

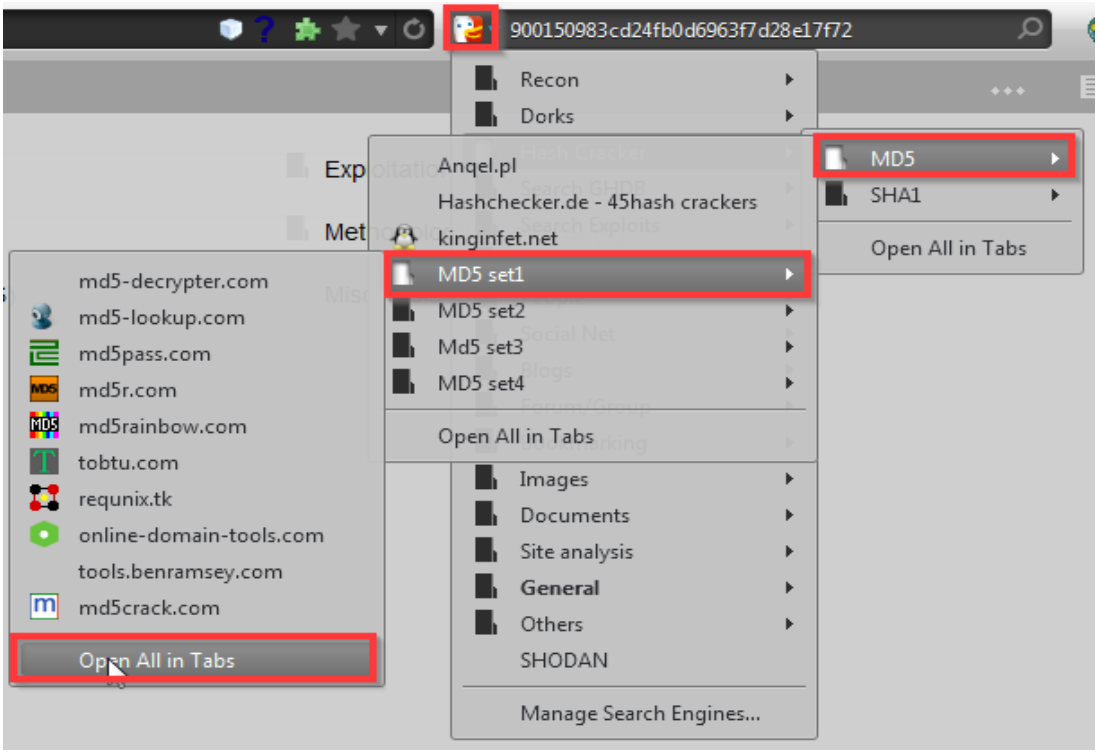


Figure 134: Running multiple online MD5 hash lookups simultaneously

This will going to search into the number of databases we selected and will give decrypted string.

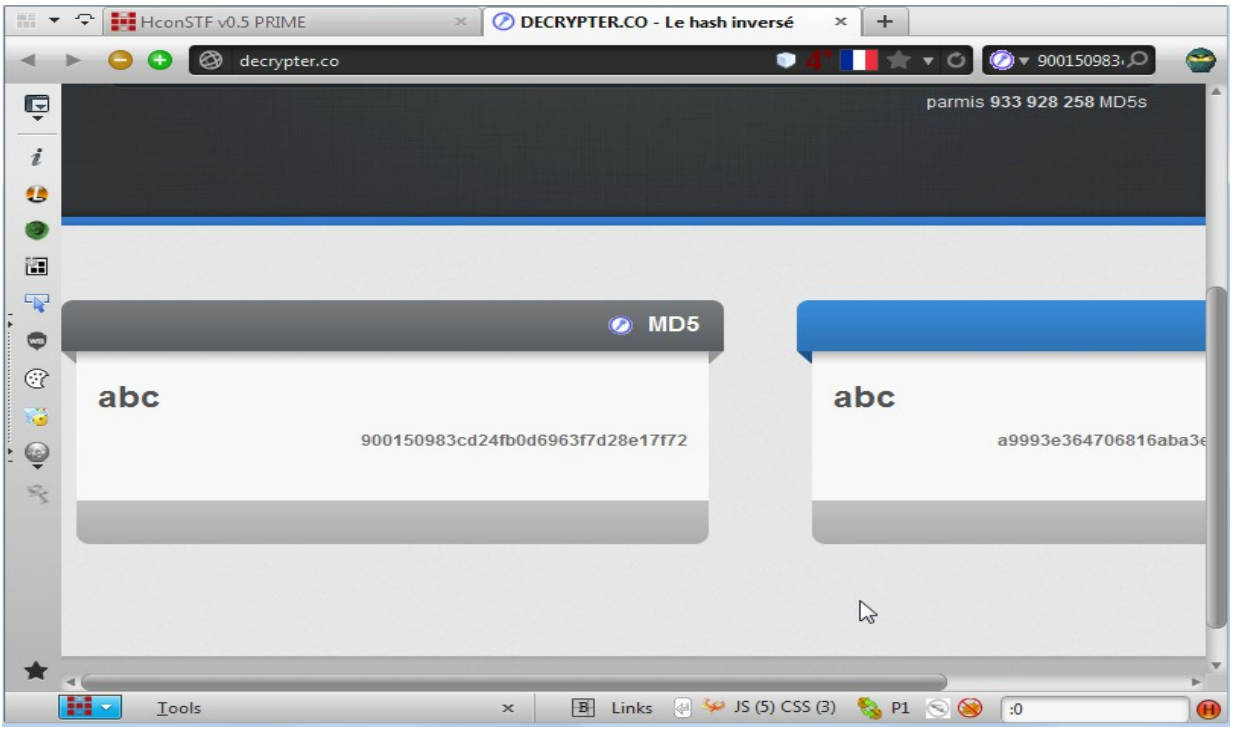


Figure 135: Plain text of hash by online database lookup

Cracking SHA1 Hashes

For cracking SHA1 there is only online hash lookup functionality is available via search aggregator plugins currently in HconSTF, which is the same method that we applied for MD5 online hash lookup.

Note: *We can run all the plugins but that will take some resource for few seconds and it is not recommended as there are 40+ database plugins for MD5 and 10 database plugins for SHA1. Some of the database plugins also supports other hash algorithms like SHA256, SHA512, MD5 variants and more.*

Chapter 7: Anonymity

In this chapter we will look it how to use its spoofing and proxy features.

7.1 User Agent Spoofing

User agent is the web client's identity that it sends with each request made to the webapp. many of the web apps/sites uses this as a decision parameter for serving a different site or version of site to that user with different user agent of their web client. Because of this kind of web app/site behavior we as webapp testers take this as parameter to test and take advantage of it whenever possible.

Advantages of spoofing user agent:

- Different version of web app/site may have vulnerabilities.
- With different user agent the target web app/site may response differently to web requests, so exposure to more content manipulation and exploitation can turn into compromise.
- When needed we can hide one of the part of our online identity that is user agent.
- Useful for browsing and bypassing weak directory listing protections like the one we see in Robots.txt which allows certain web clients to browse the directories.

spoofing user agent of HconSTF, in our request headers the default user agent is:

User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:17.0) Gecko/20100101 Firefox/17.0

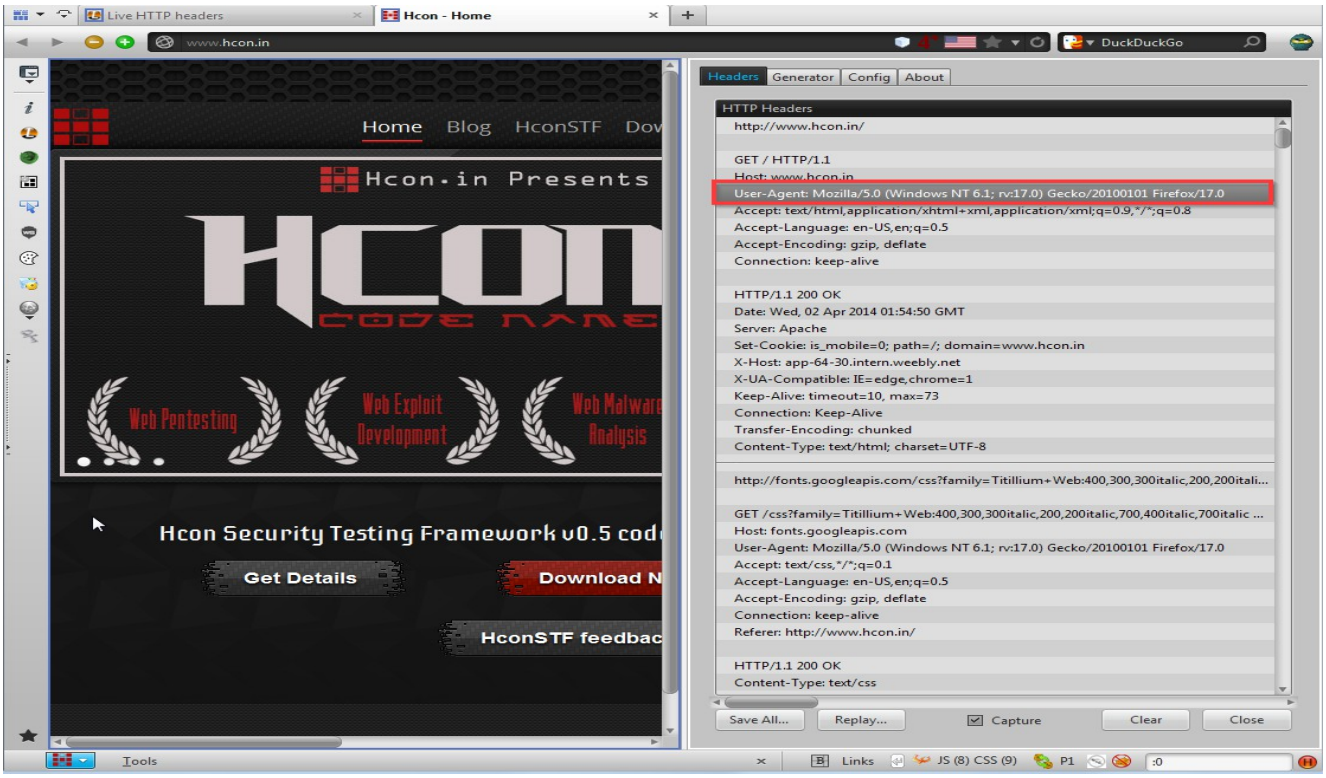


Figure 136: Default user agent of HconSTF

Click on the gray earth icon on the sidebar and select the new user agent we want to use.

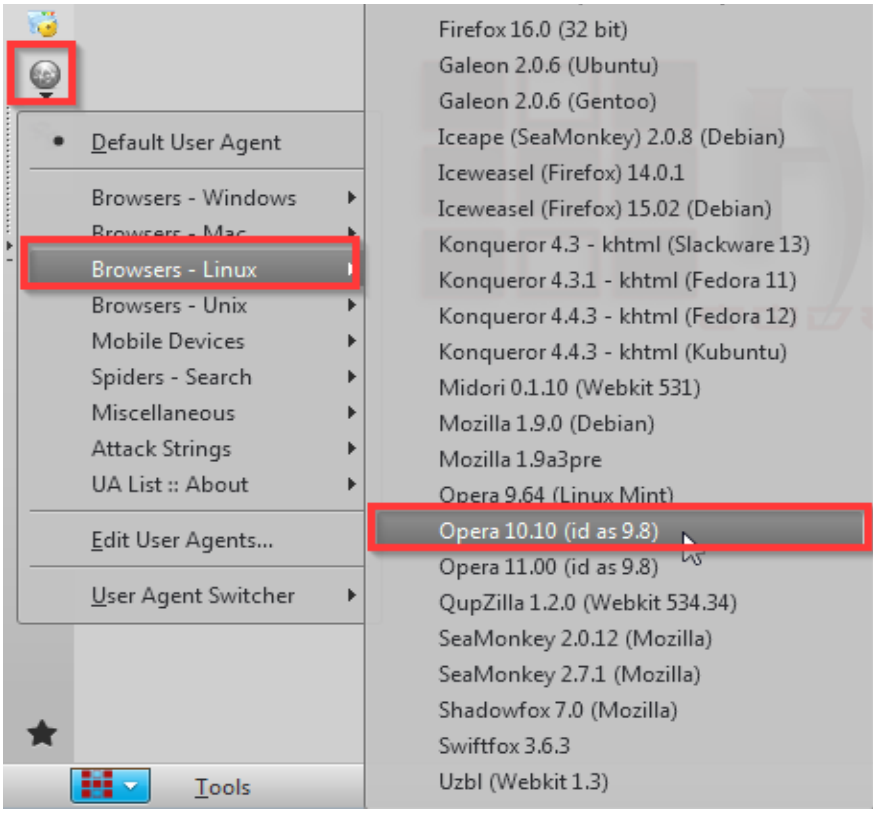


Figure 137: Selecting new user agent

we can also access the same menu from Hmenu → Anonymity → Default User Agent

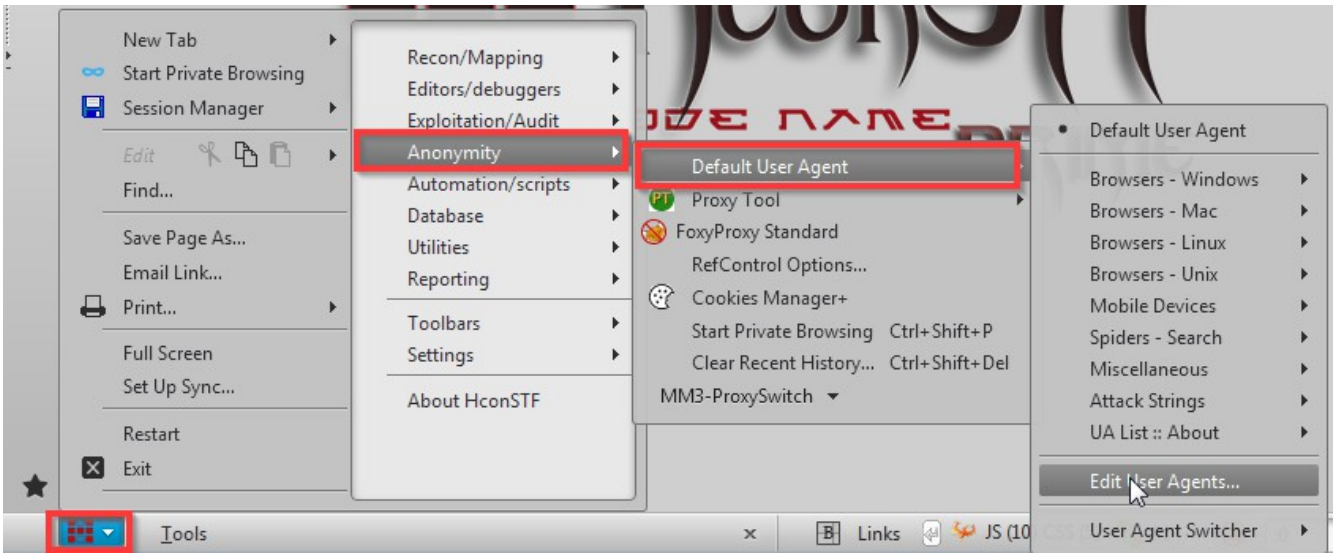


Figure 138: User agent switcher in Hmenu

Select new user agent as opera on linux and reload the Hcon.in page, check the user agent in the request headers.

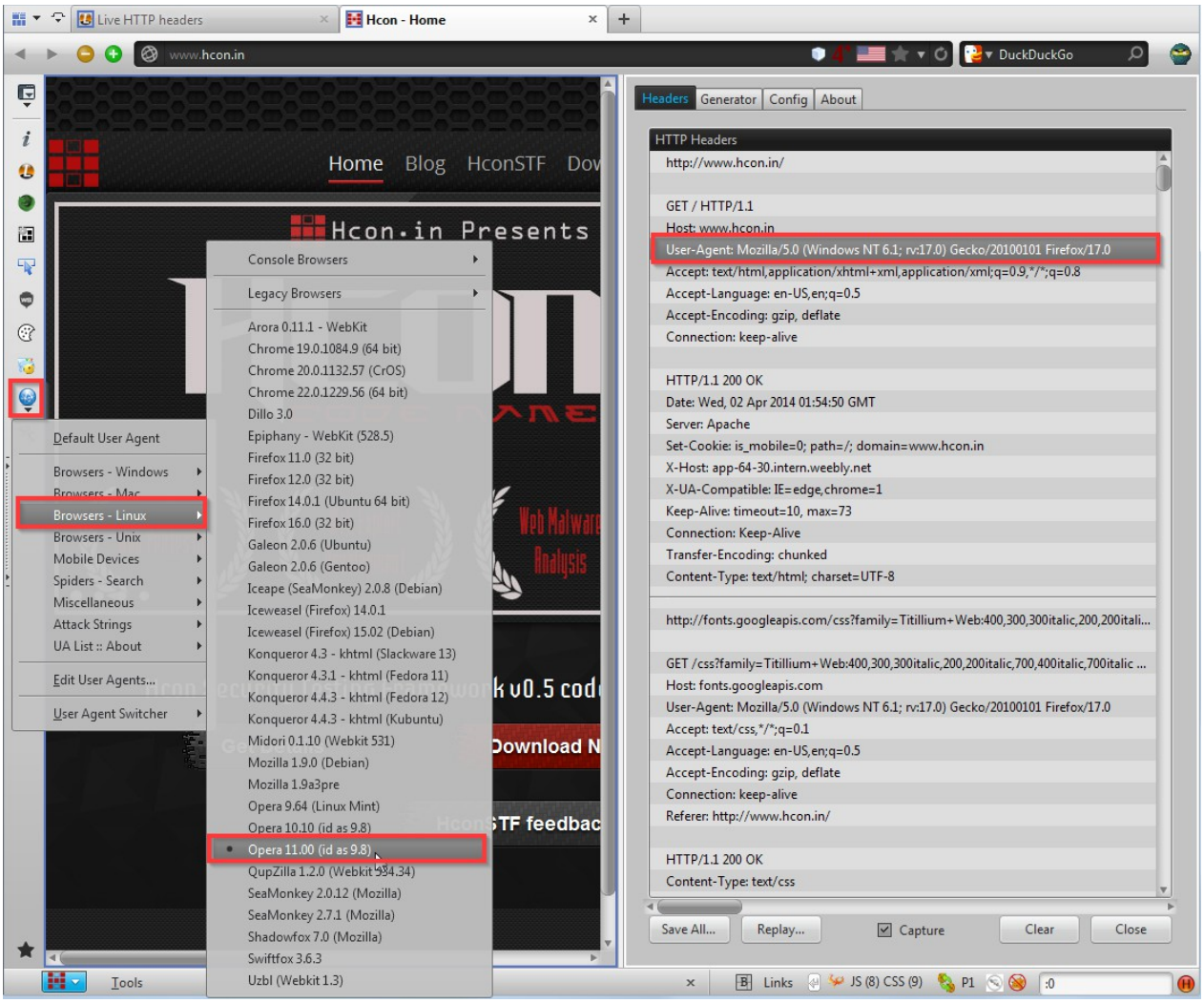


Figure 139: Old and new user agent

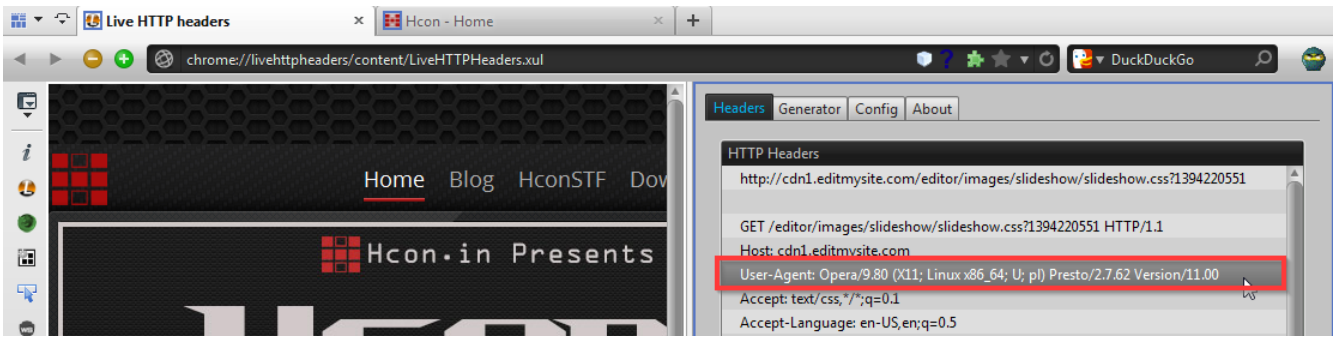
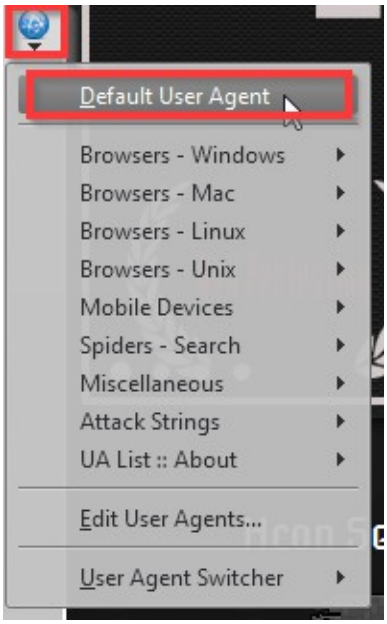


Figure 140: New changed user agent

As we can see new changed user agent is:

User-Agent: Opera/9.80 (X11; Linux x86_64; U; pl) Presto/2.7.62 Version/11.00

For restoring the default user agent back just click on 'Default User Agent' from sidebar menu.



Note: *For easy identification of our current user agent notice that whenever the user agent is default the earth icon is gray once it is changed to spoofed user agent the icon turns blue.*

7.2 Header Spoofing

Whenever we visit any site or use web application, we request data by sending HTTP requests to the server. This HTTP requests uses different HTTP headers.

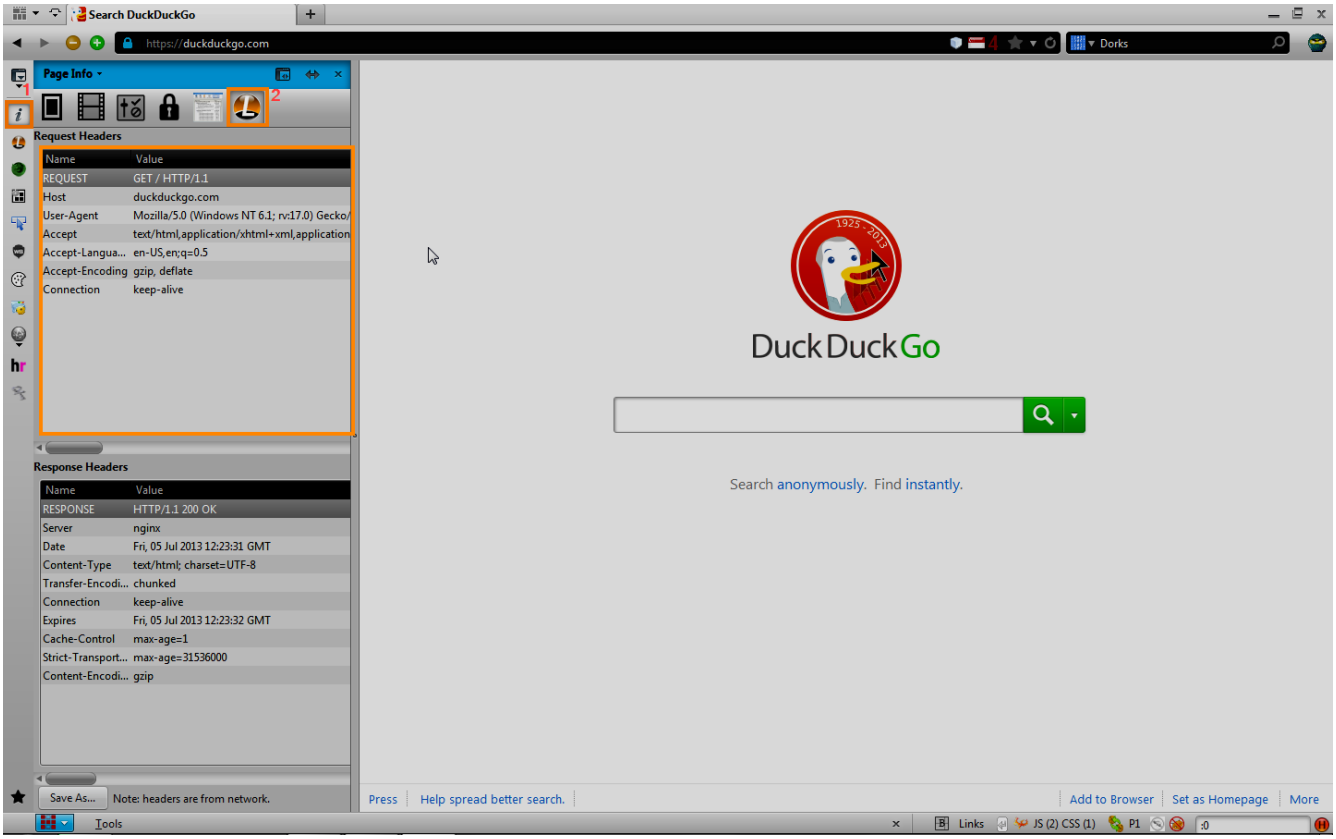


Figure 141: Default request headers

One interesting thing about this headers is that some of them reveals our IP address to the server by sending it in the HTTP headers. The responsible headers for this are,

- X-Forwarded-For – Shows origins of the request sender or even from any HTTP proxy.
- Client-IP – Shows the IP address of the request sender.
- Via – Sends IP address of proxies used.

But instead of revealing the information or just making it blank and sending it to the webapp, we can spoof it and use any IP to send it to webapp easily by HconSTF.

Let us do that using HonSTF, See the location in the image and right click on the icon

Status bar → right click on Ipflood → Preferences

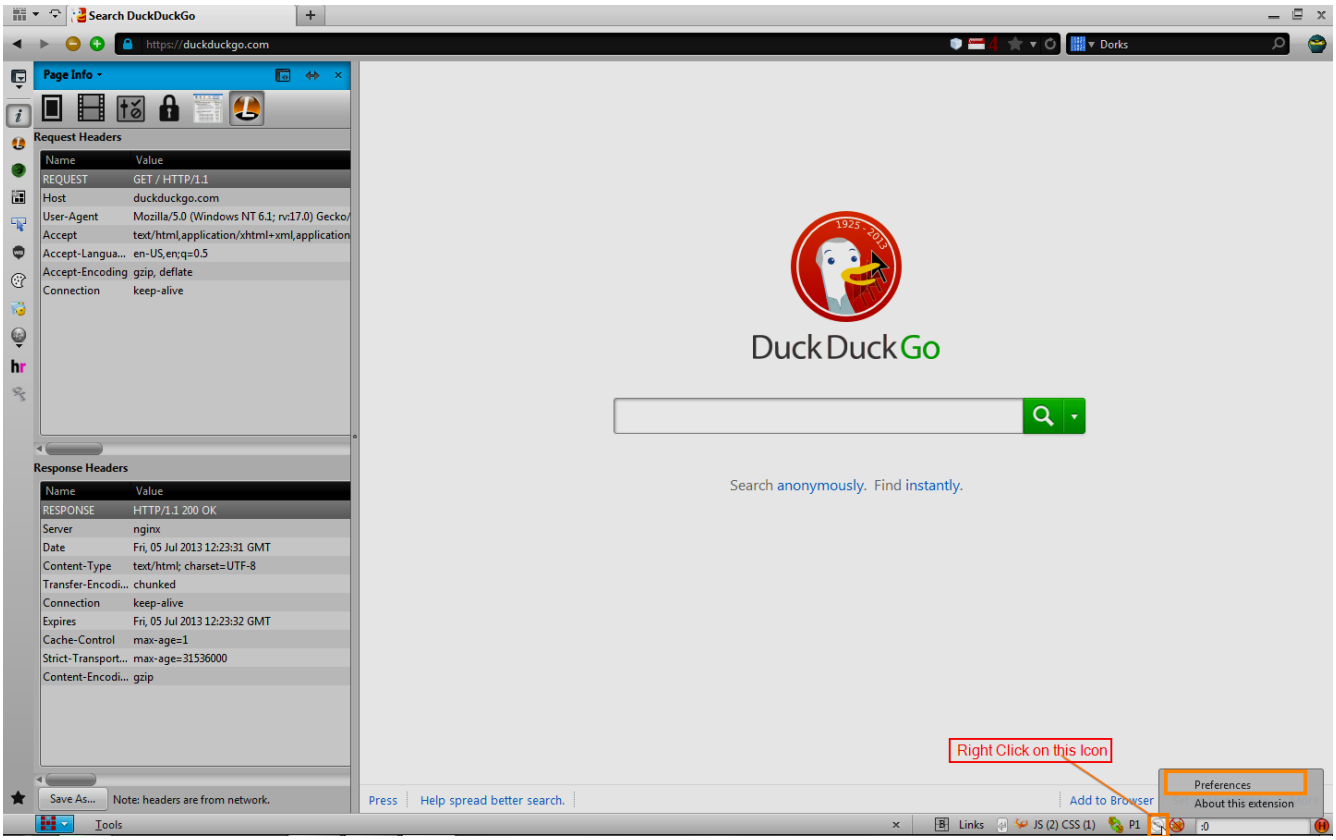


Figure 142: Opening IPflood preferences

By using this we will add custom headers into the HTTP request which will misguide the server.

Lets we configure it to use the custom headers we want.

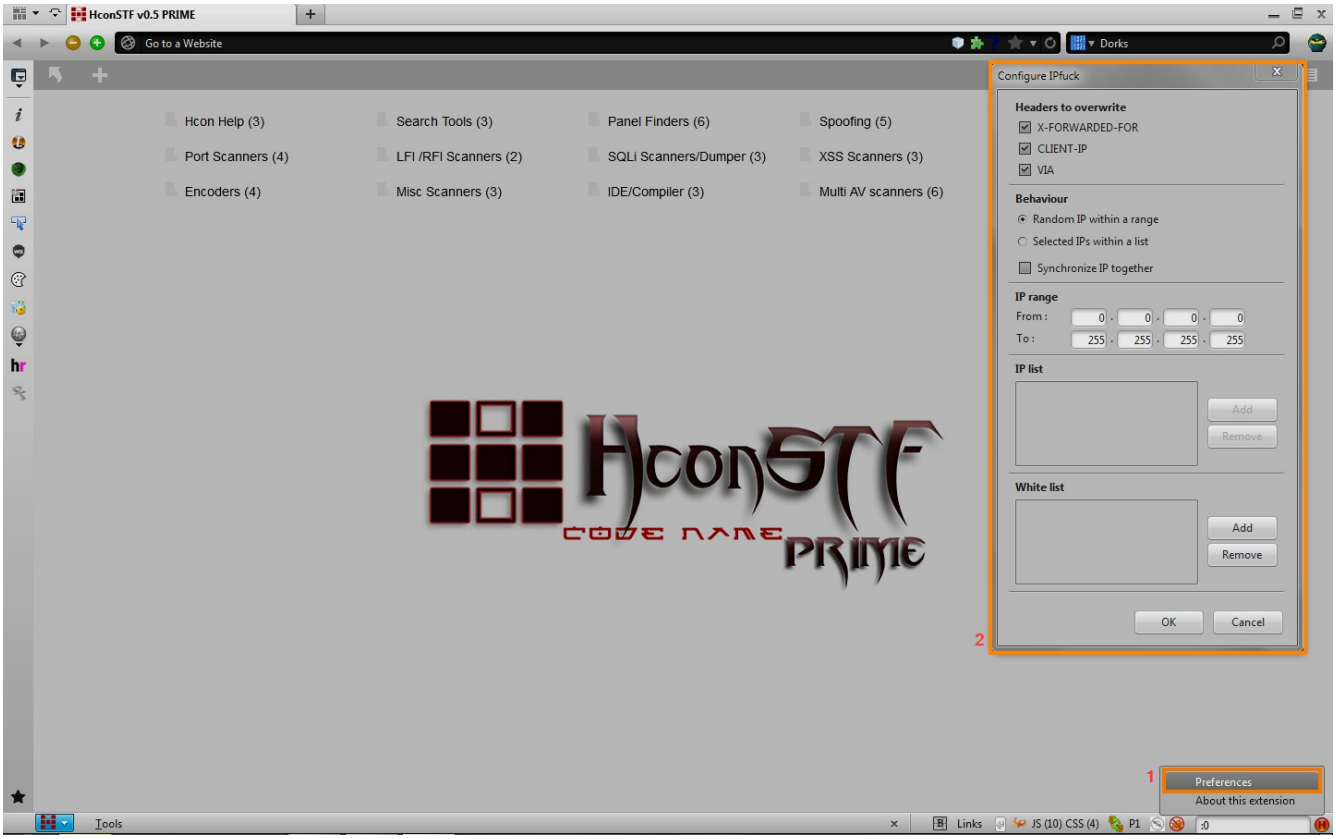


Figure 143: IPflood preference window

Right click the icon and open preferences can be configured to use,

- Random range of IP Address
- Provide a list of IP address to use

Now lets configure as we want and activate tool to see the results

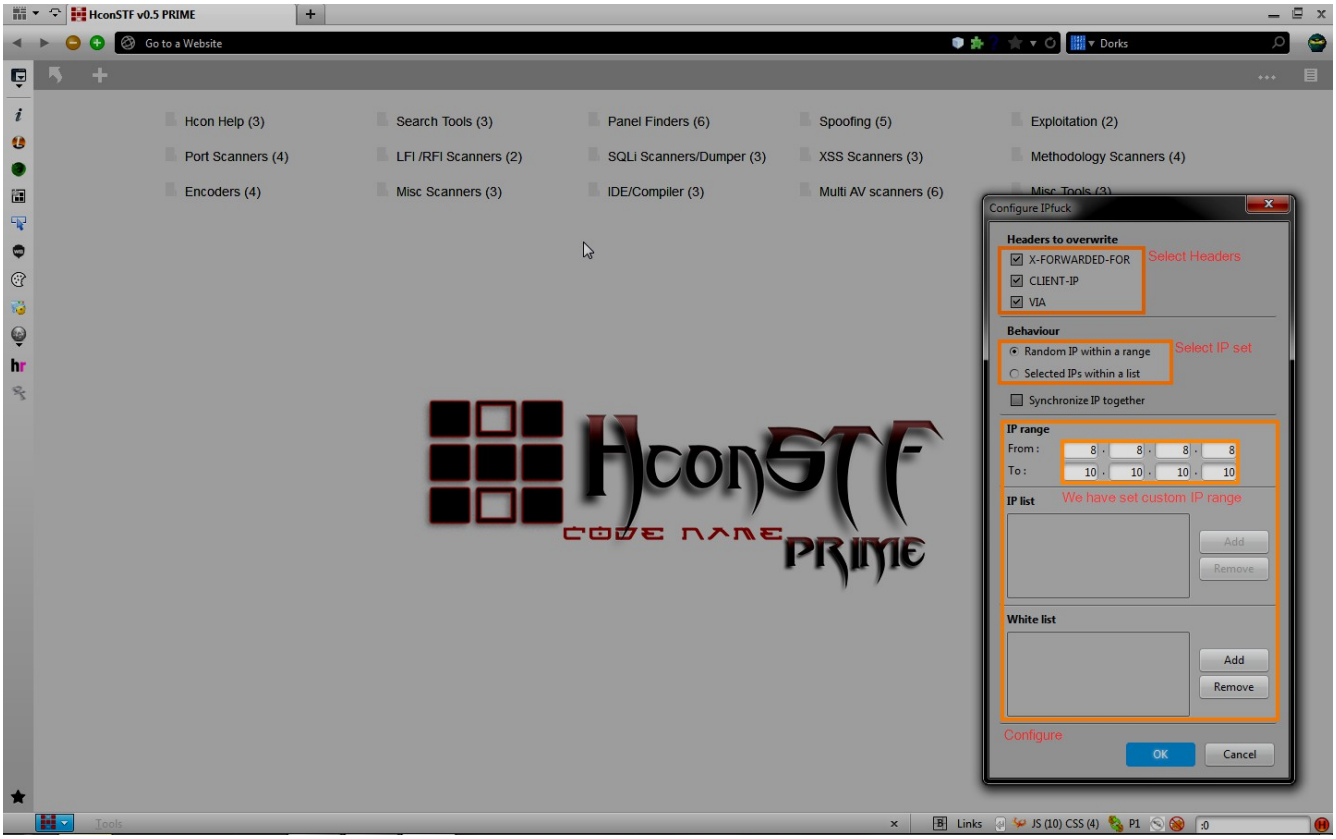


Figure 144: Configured spoofing options

1. We will going to use all the headers to send, so selecting all the type of HTTP headers.
2. Choosing the random IP address range and adding range from 8.8.8.8 to 10.10.10.10
3. Save it by clicking 'OK' and activate the configurations by just left clicking on the icon, it will turn dark.

Now to test it just refresh the page and open the header reader as shown in the figure below.

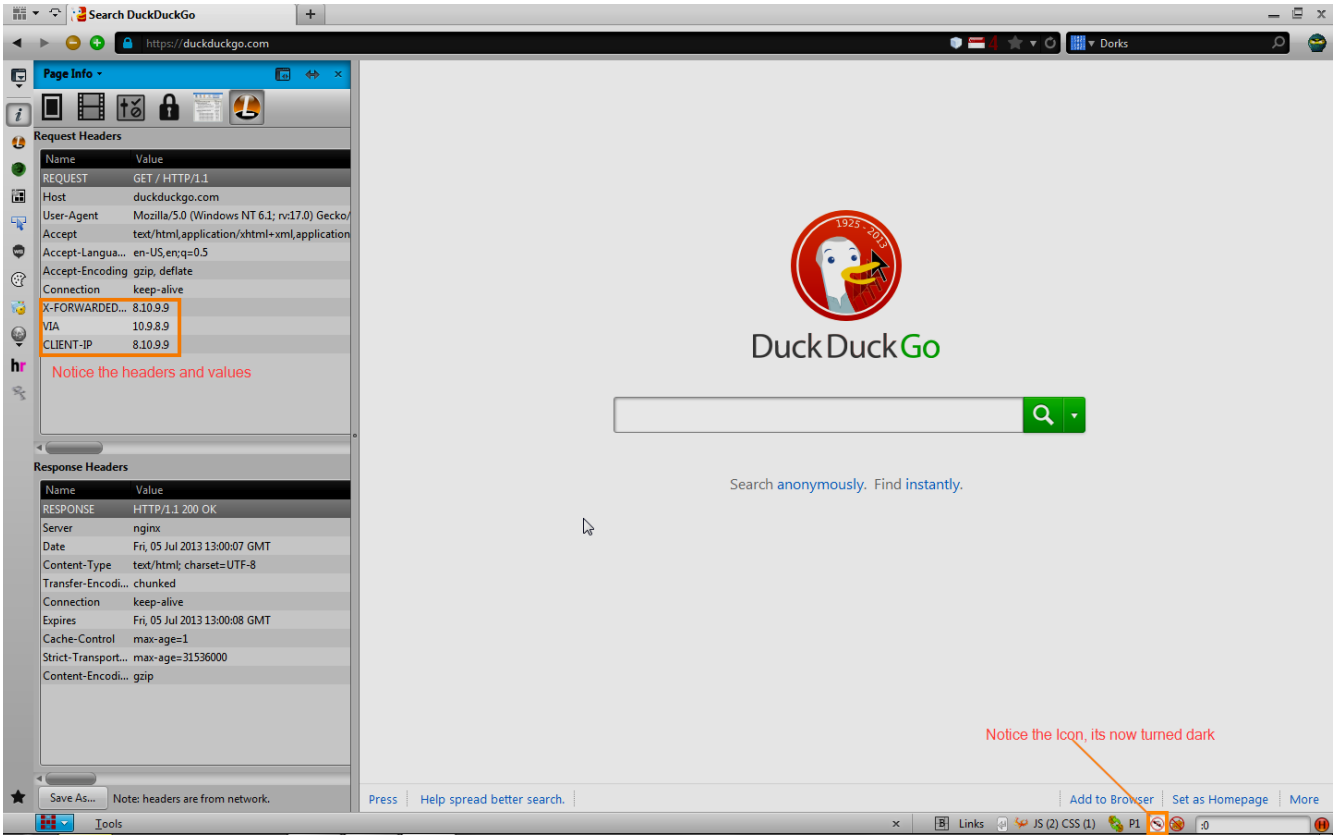


Figure 145: Spoofed IP fields in request header

7.3 Darknets & Proxies

HconSTF supports many types of decoys for different purposes in our pentesting assessment.

types of decoys supported are,

Darknets:

- Tor
- AdvTOR
- I2P

For using any of the above decoys we can connect and switch between all of them very quickly as HconSTF is preconfigured for using this. what we have to do is just run the instance of any of above and connect to it.

Lets see how to use HconSTF with Tor,

Run vidalia or Tor-browser bundle instance, connect HconSTF with single click configuration.

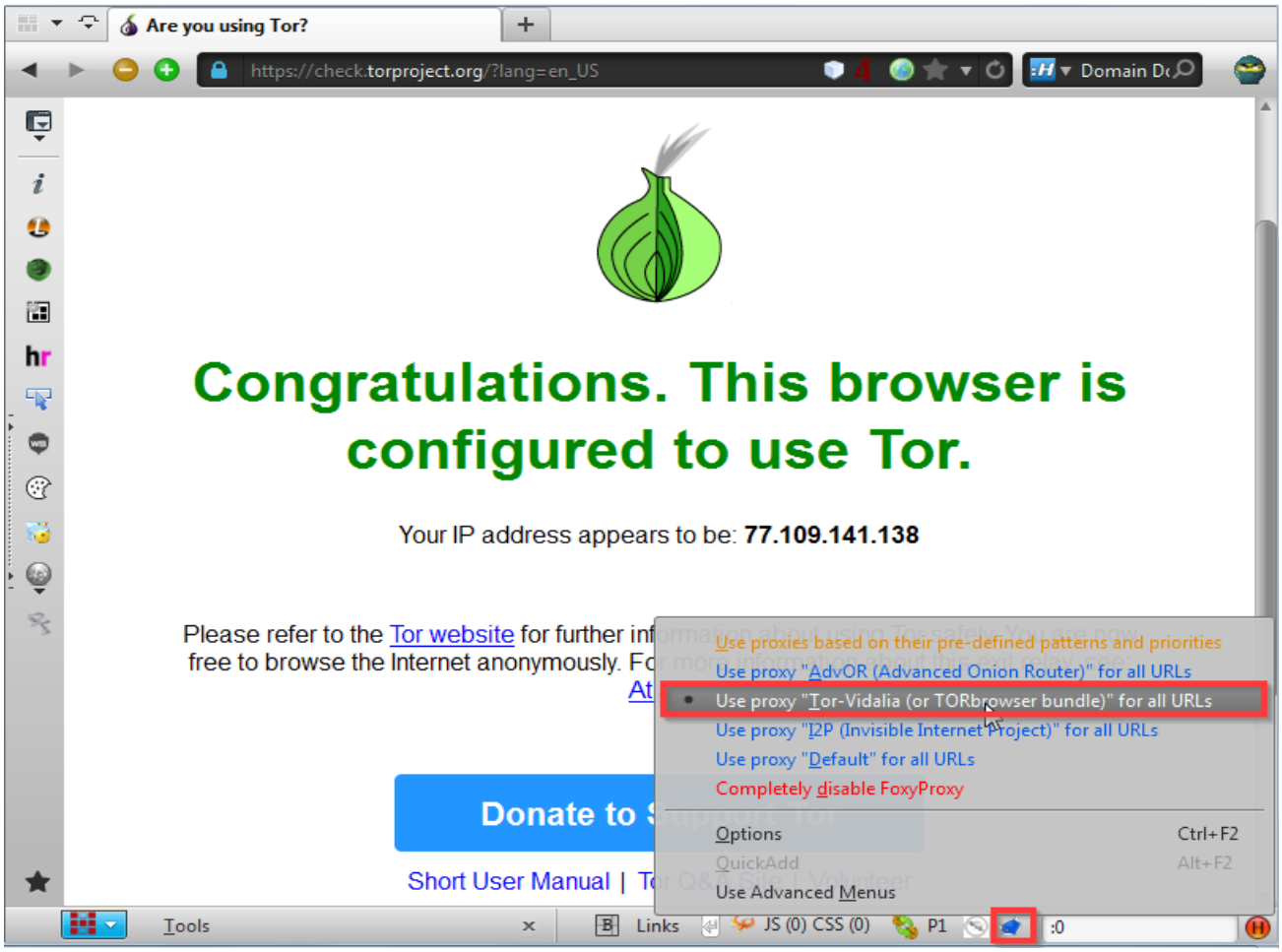

Are you using Tor?
https://check.torproject.org/?lang=en_US
Congratulations. This browser is configured to use Tor.
Your IP address appears to be: 77.109.141.138
Please refer to the Tor website for further inf
free to browse the Internet anonymously. Fo
At
Donate to
Short User Manual
Use proxies based on their pre-defined patterns and priorities
Use proxy "AdvOR (Advanced Onion Router)" for all URLs
Use proxy "Tor-Vidalia (or TORbrowser bundle)" for all URLs
Use proxy "I2P (Invisible Internet Project)" for all URLs
Use proxy "Default" for all URLs
Completely disable FoxyProxy
Options Ctrl+F2
QuickAdd Alt+F2
Use Advanced Menus
Tools
Links
JS (0) CSS (0)
P1

Figure 146: Connecting HconSTF with Tor

The same way we can connect AdvTor and I2P and it is very easy to use with HconSTF.

Proxies:

- Http
- Https
- Socks 4
- Socks 5

Using this kind of decoys are also very easy as there are two ways do it, using the foxyproxy tool the same tool that we used for using darknets.

Status bar → Foxyproxy → Options

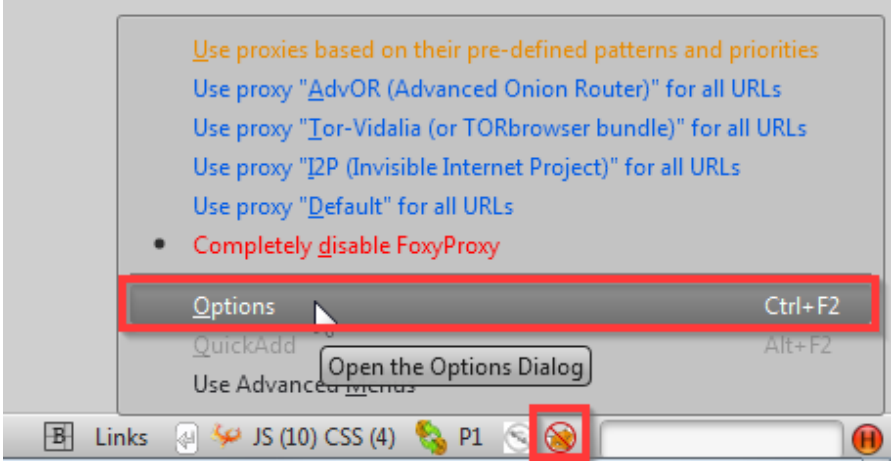

Use proxies based on their pre-defined patterns and priorities
Use proxy "AdvOR (Advanced Onion Router)" for all URLs
Use proxy "Tor-Vidalia (or TORbrowser bundle)" for all URLs
Use proxy "I2P (Invisible Internet Project)" for all URLs
Use proxy "Default" for all URLs
Completely disable FoxyProxy
Options Ctrl+F2
QuickAdd Alt+F2
Open the Options Dialog
Links
JS (10) CSS (4)
P1

Figure 147: Editing configurations

Click 'Add new proxy'

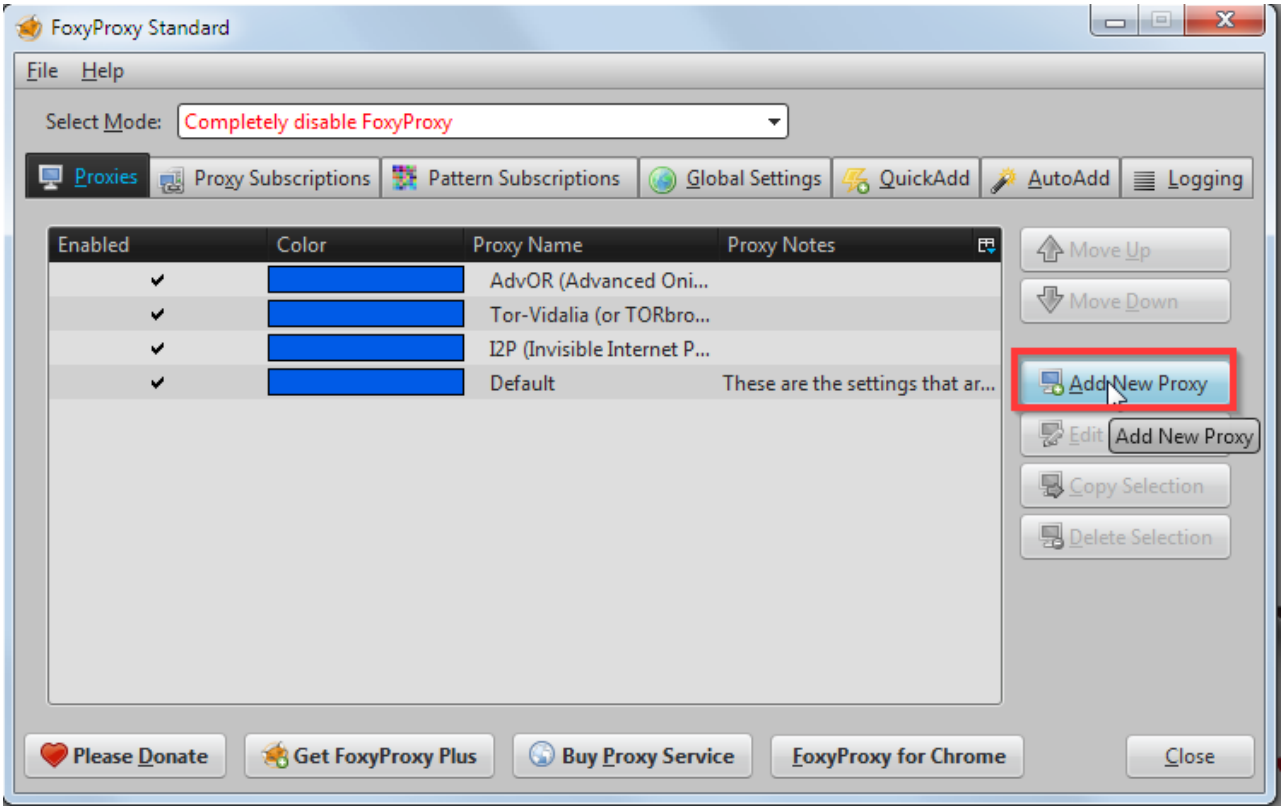


Figure 148: Adding new proxy

Now add the proxy type we want to use http, https, socks 4/5 and save it.

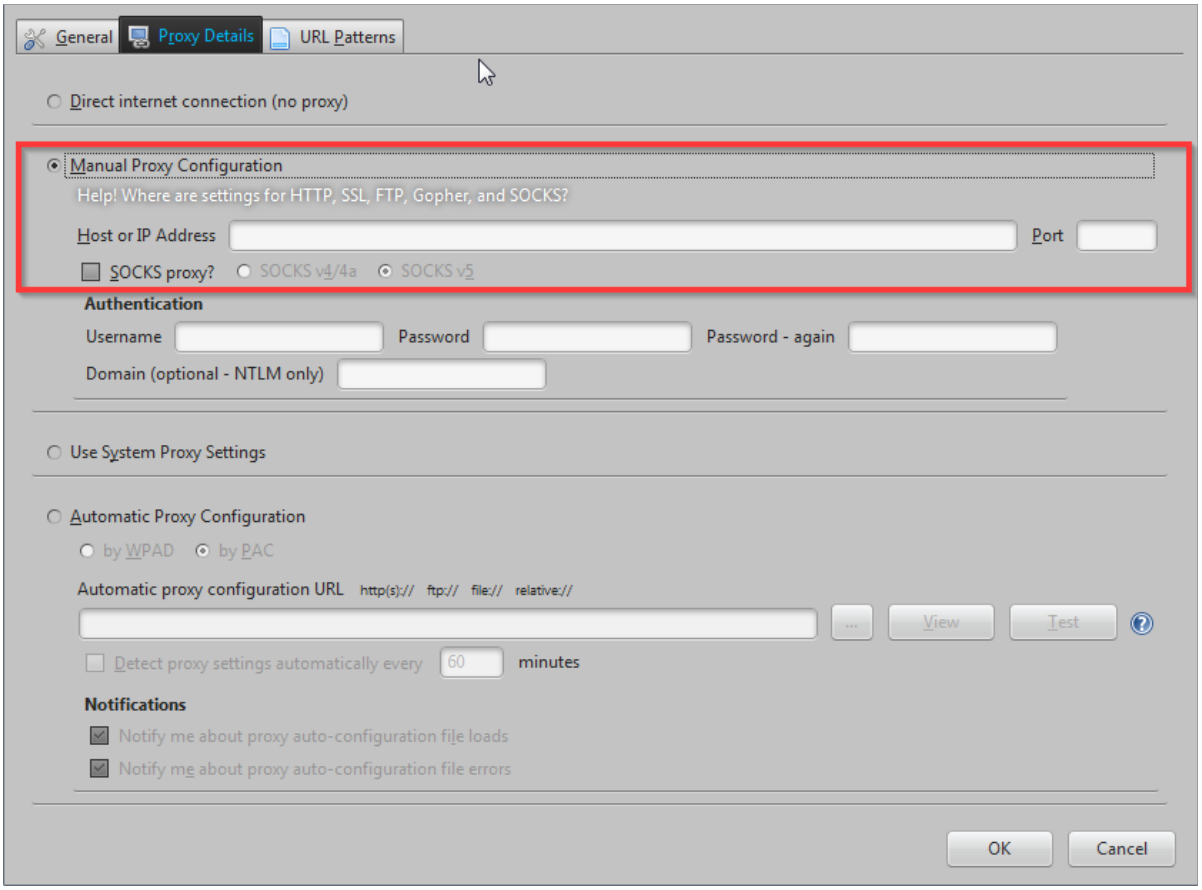


Figure 149: Setting up new proxy

for using our configured proxy and switching between each other use the foxyproxy menu to select it.

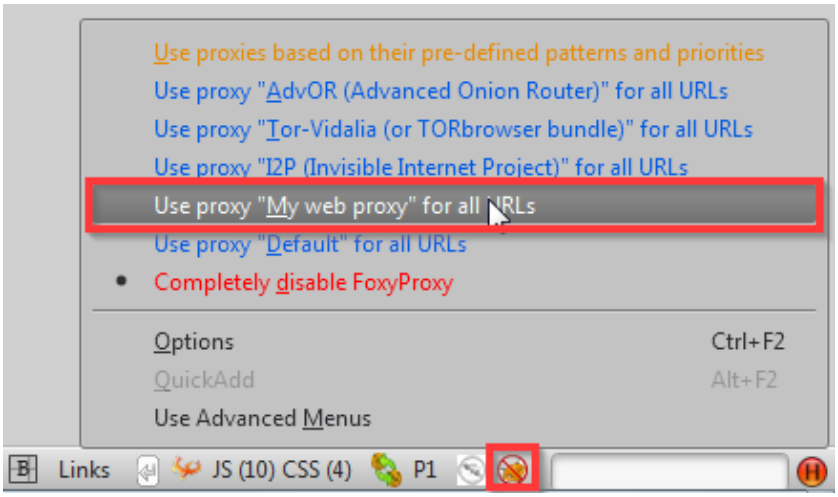

Use proxies based on their pre-defined patterns and priorities
Use proxy "AdvOR (Advanced Onion Router)" for all URLs
Use proxy "Tor-Vidalia (or TORbrowser bundle)" for all URLs
Use proxy "I2P (Invisible Internet Project)" for all URLs
Use proxy "My web proxy" for all URLs
Use proxy "Default" for all URLs
Completely disable FoxyProxy
Options
Ctrl+F2
QuickAdd
Alt+F2
Use Advanced Menus
Links
JS (10) CSS (4)
P1

Figure 150: Selecting the new proxy created

It does support other types of decoys like VPN.

Another way of using this type of proxies is to enter IP:port in empty box in status bar

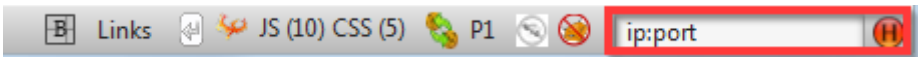


Figure 151: Quickly adding proxies

Click on the red circle H icon as it will turn green that means our proxy is active

Figure 152: Quickly added http proxy

Other then this we can import our own proxy list into HconSTF by,

Right click on the circle H icon in stratus bar and click on 'Import proxies'

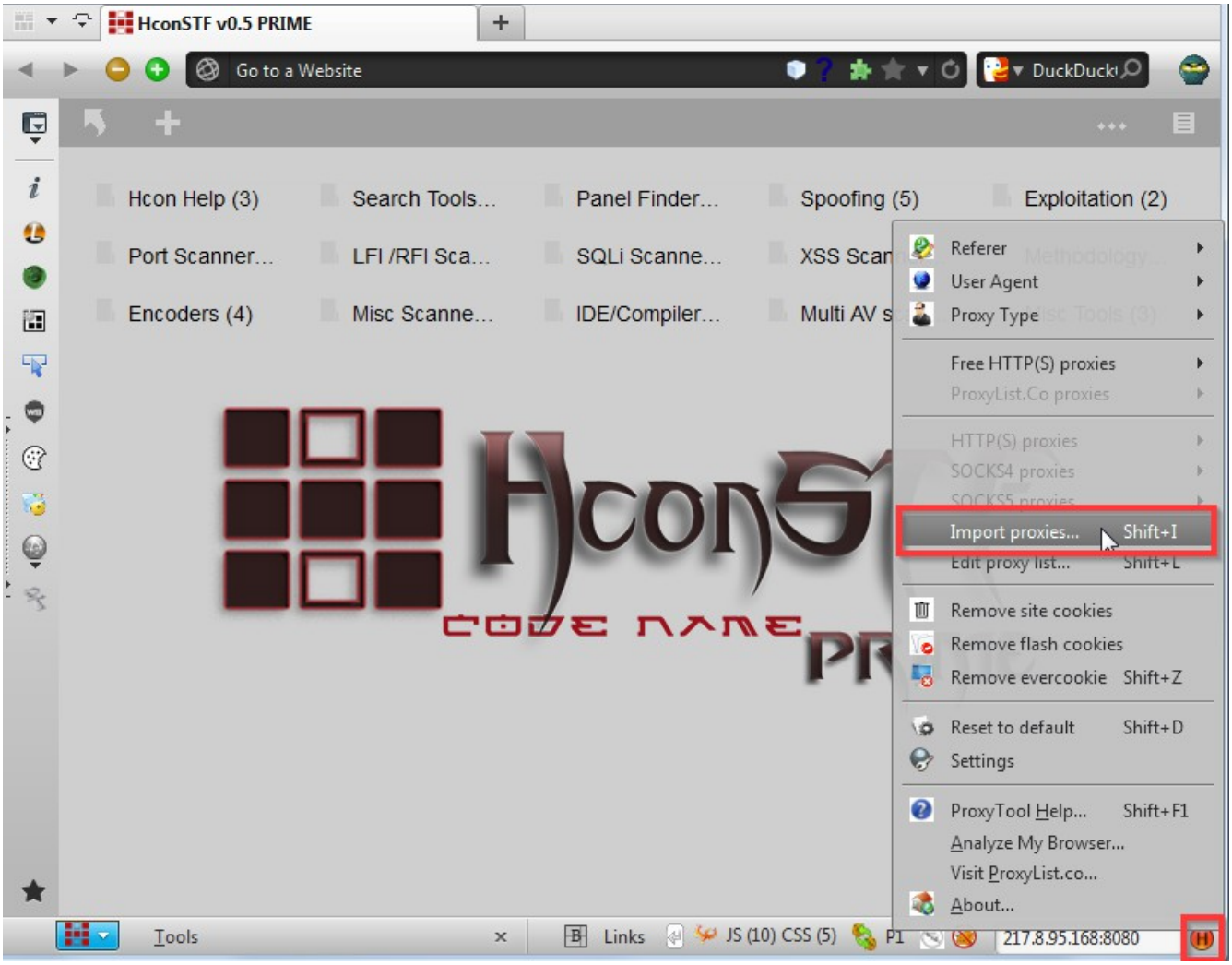


Figure 153: Importing new proxies

Paste any type of proxies into that box and select the type of it as each individual IP:port combination can be defined as http, socks 4, socks 5.

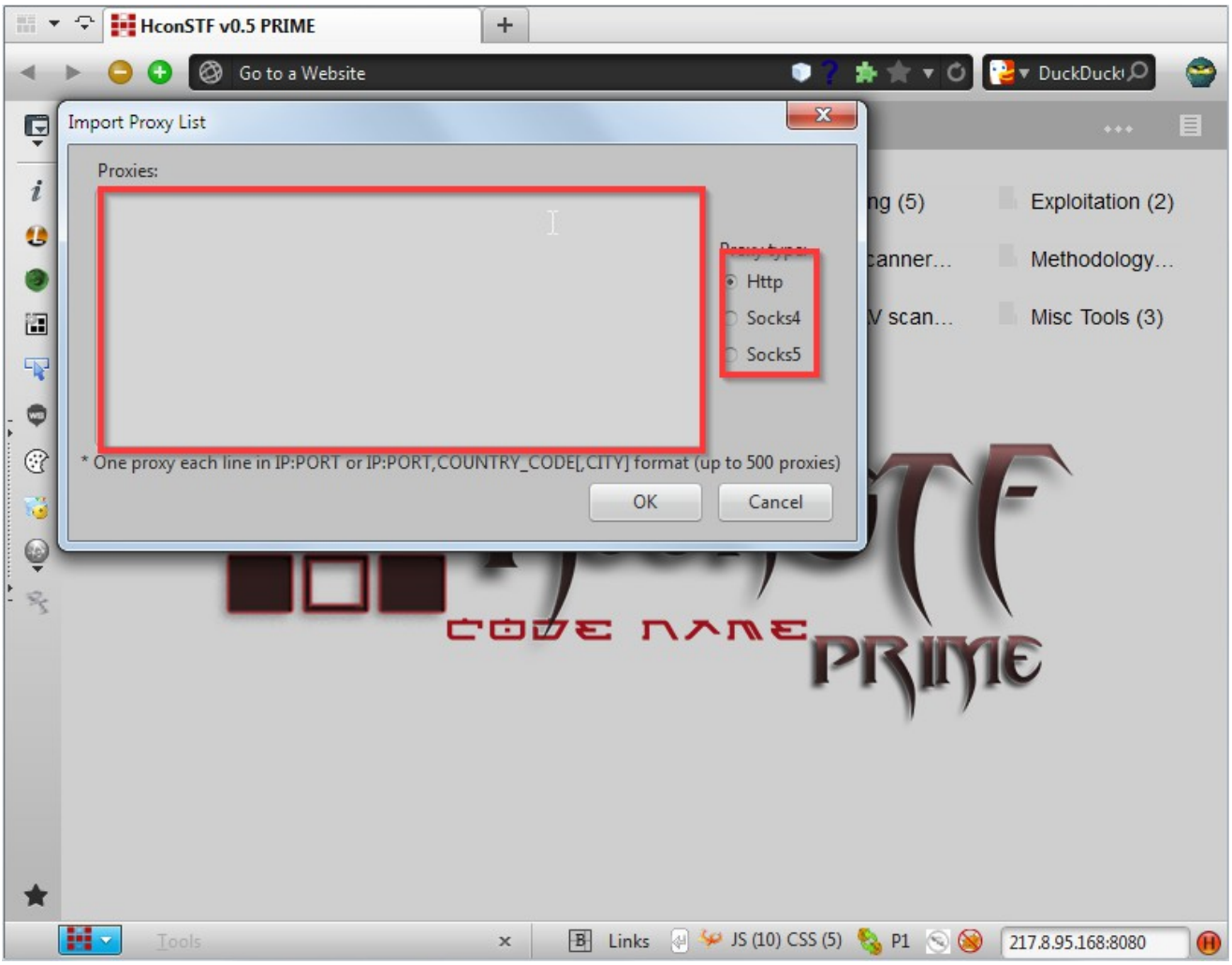


Figure 154: Defining type of imported proxies

Now we can use from the list from the same menu.

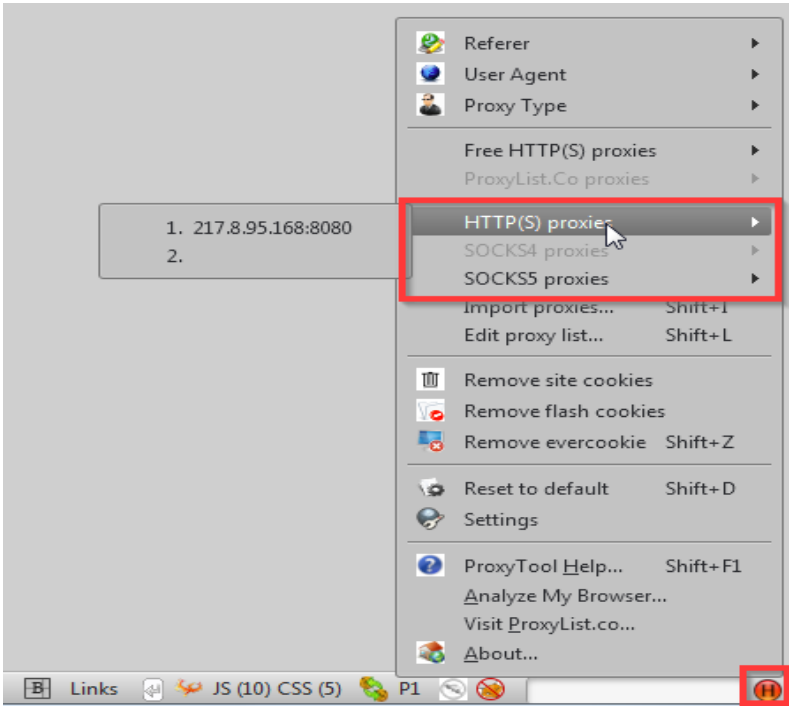


Figure 155: Selecting from imported proxies

Note: *When using any kind of decoys make sure to block scripts globally in HconSTF.*

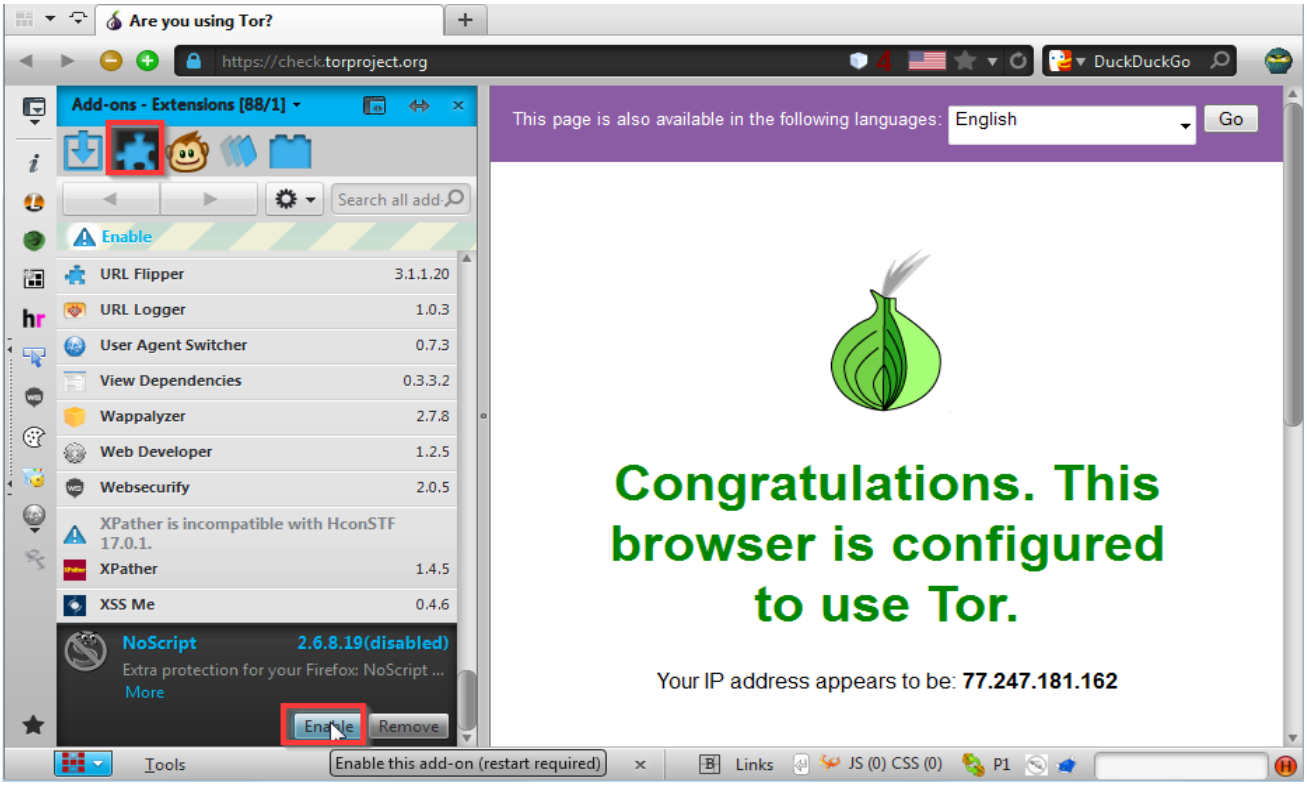


Figure 156: Enabling Noscript

Goto Hmenu → Settings → Add-ons, go down in the list and enable 'NO Script', Restart HconSTF.

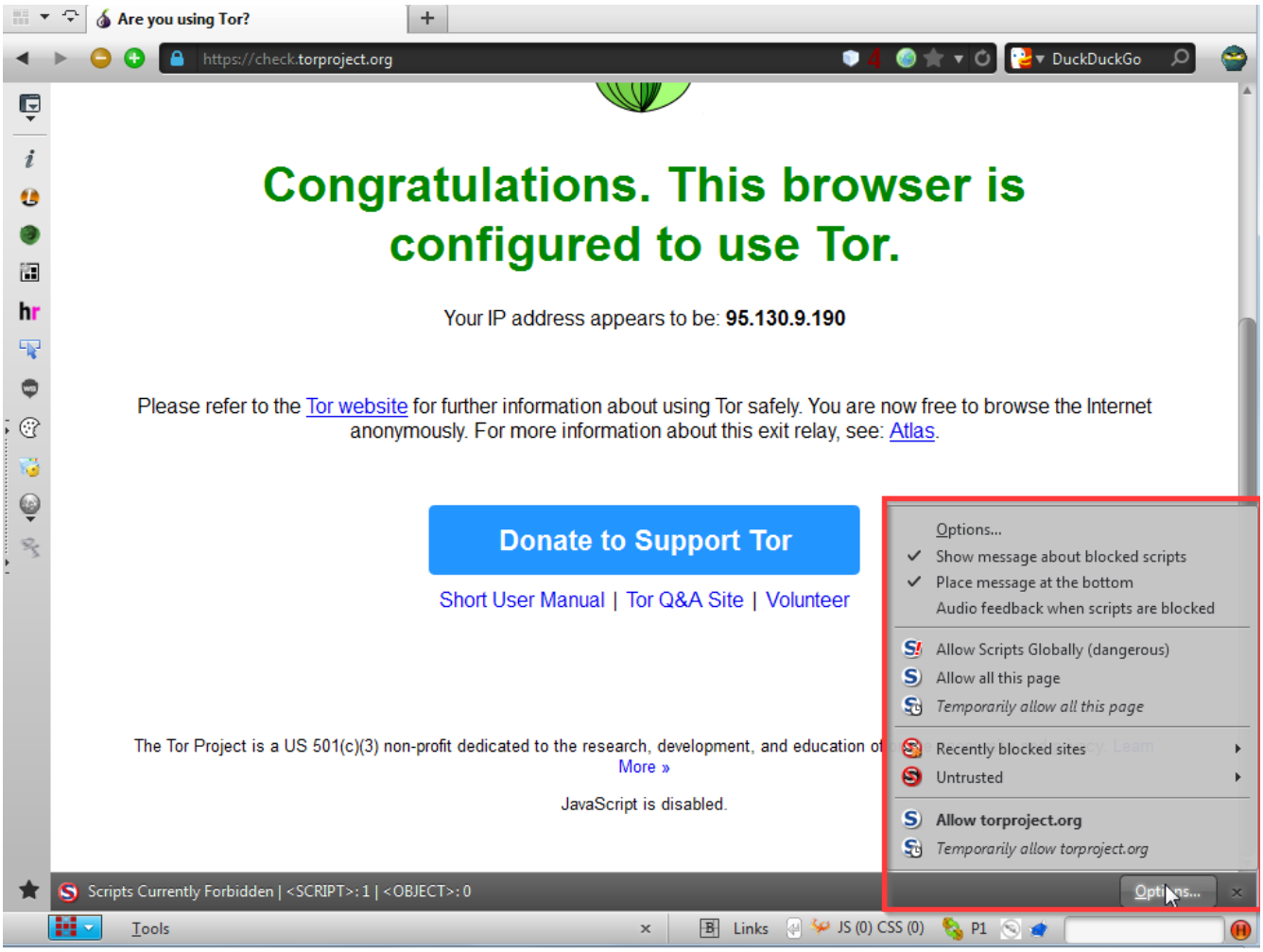

Are you using Tor?
https://check.torproject.org
DuckDuckGo
Congratulations. This browser is configured to use Tor.
Your IP address appears to be: 95.130.9.190
Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: Atlas.
Donate to Support Tor
Short User Manual | Tor Q&A Site | Volunteer
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of
More »
JavaScript is disabled.
Options...
Show message about blocked scripts
Place message at the bottom
Audio feedback when scripts are blocked
Allow Scripts Globally (dangerous)
Allow all this page
Temporarily allow all this page
Recently blocked sites
Untrusted
Allow torproject.org
Temporarily allow torproject.org
Scripts Currently Forbidden | <SCRIPT>: 1 | <OBJECT>: 0
Options...
Tools
Links
JS (0) CSS (0)
P1

Figure 157: Allowing scripts to run or not

After enabling it we can control which JavaScript can run or not.

This provides extra layer of protection when using decoys but when we are testing a webapp which is highly based on JavaScript then this can break the webapp's functionality.

Chapter 8: Connecting with Other Tools

In this chapter we will look at conneting HconSTF with other tools and get the most out of it.

8.1 Custom Tool on IPprotocols

Other then the inbuilt tools in HconSTF we can also setup external tools to use directly from HconSTF. any tool which takes IP address in argument as target can be used in this type of setup, for this section we will going to use the default configuration of tools,

- Nmap
- Remote desktop
- SSH client
- VNC client
- Telnet
- Ping

Download nmap, ultravnc, putty by using the links below, create a directory named "Tools" under HconSTF directory.

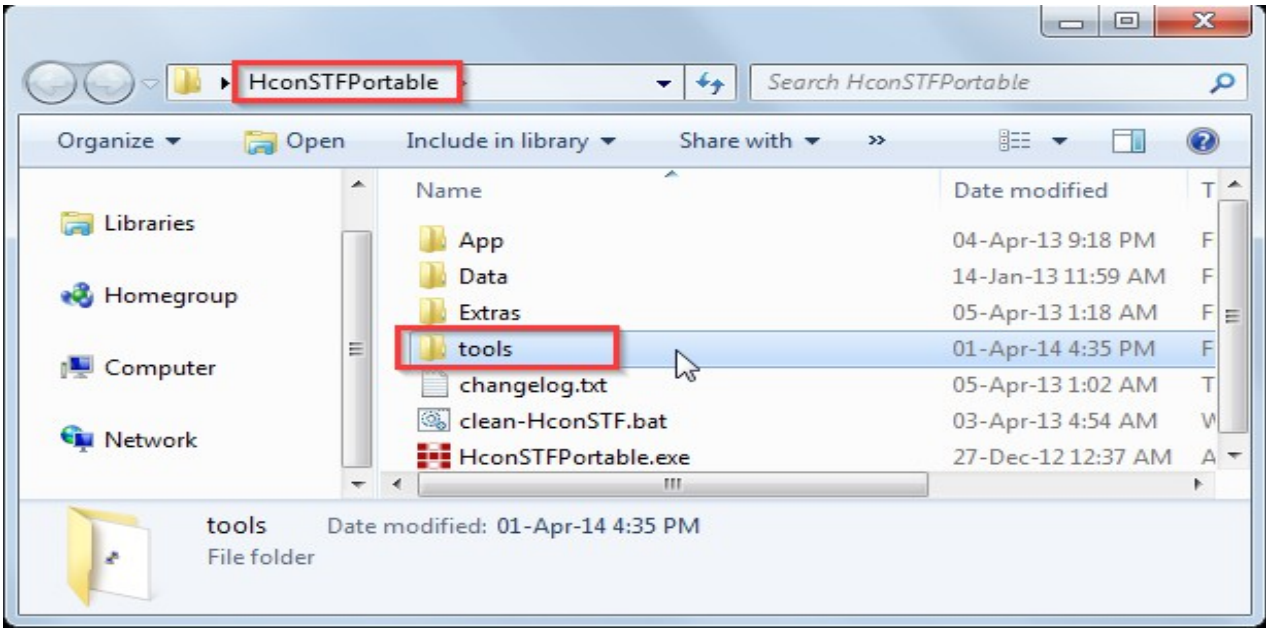


Figure 158: Adding new tools directory

Extract all the zipped archives into the sub directories in tools directory.

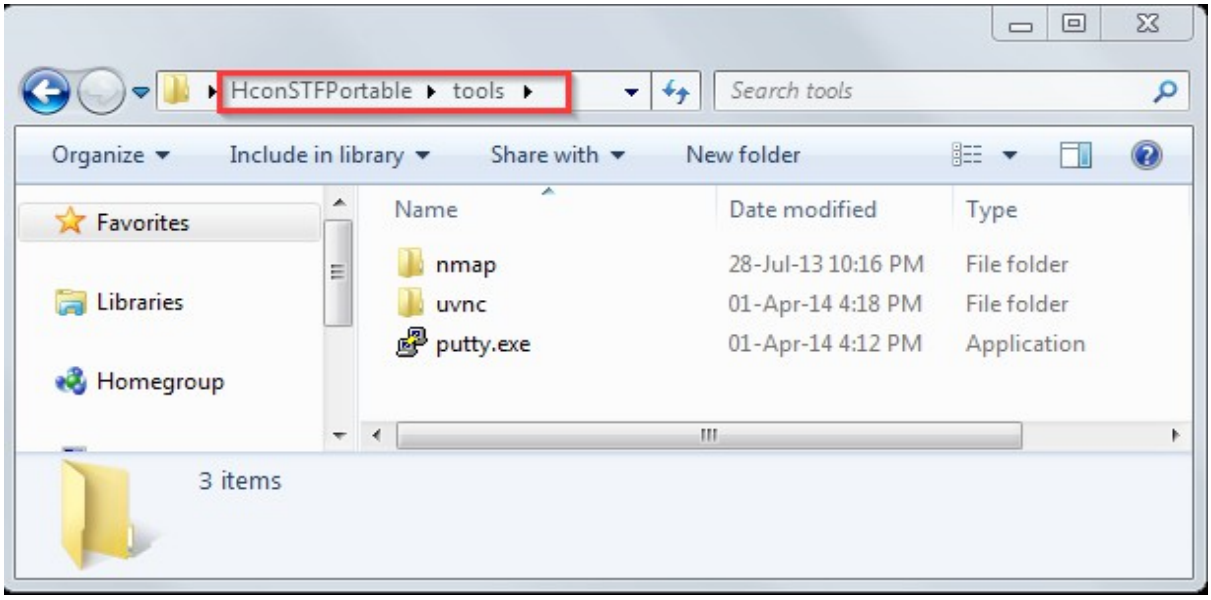


Figure 159: Arrangements in Tools directory

Now start HconSTF and open Hmenu → Settings → IPprotocols → Preferences

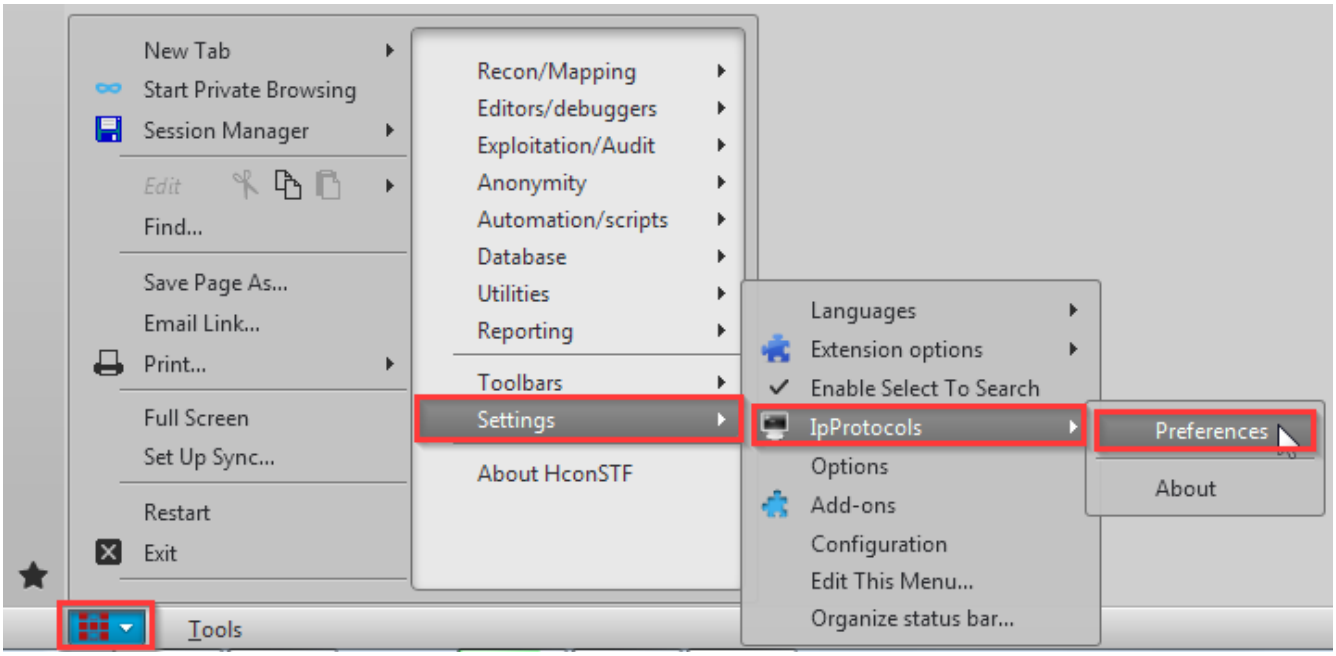


Figure 160: IPprotocols preferences

According to our operating system select either windows or linux.

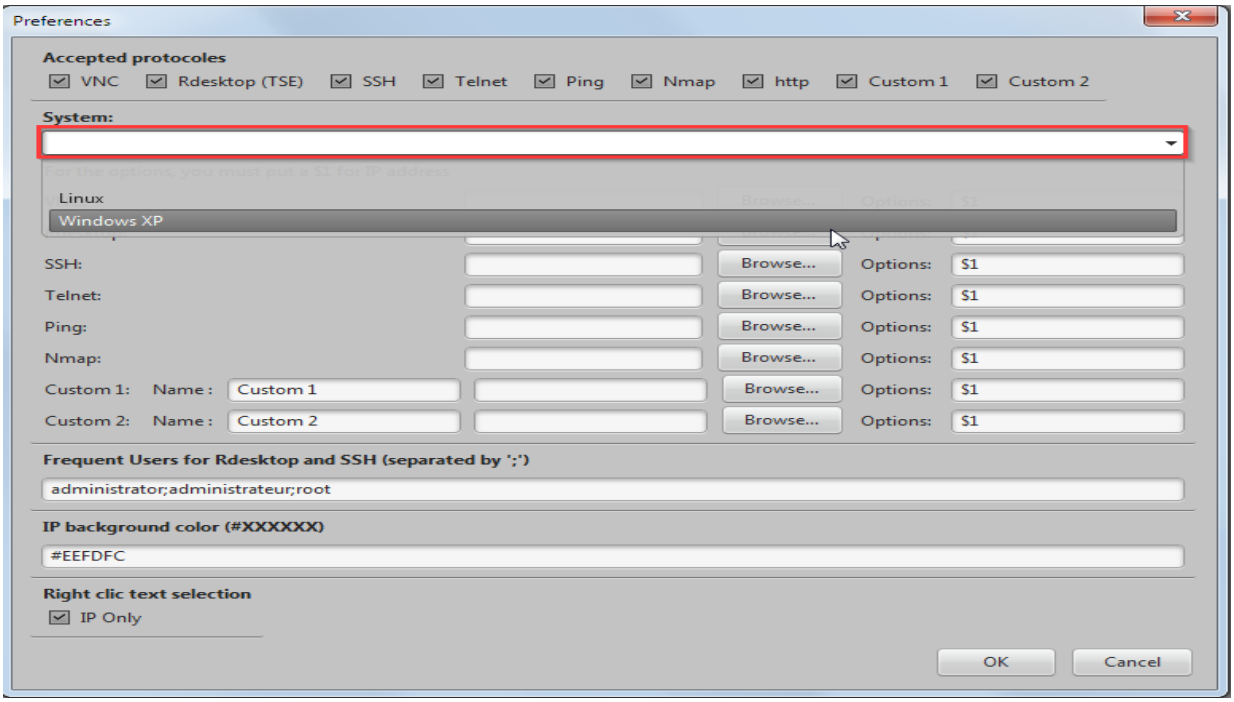


Figure 161: Selecting Operating system for tools setup

For this guide we have chosen windows XP and added absolute path to the individual tool's executable.

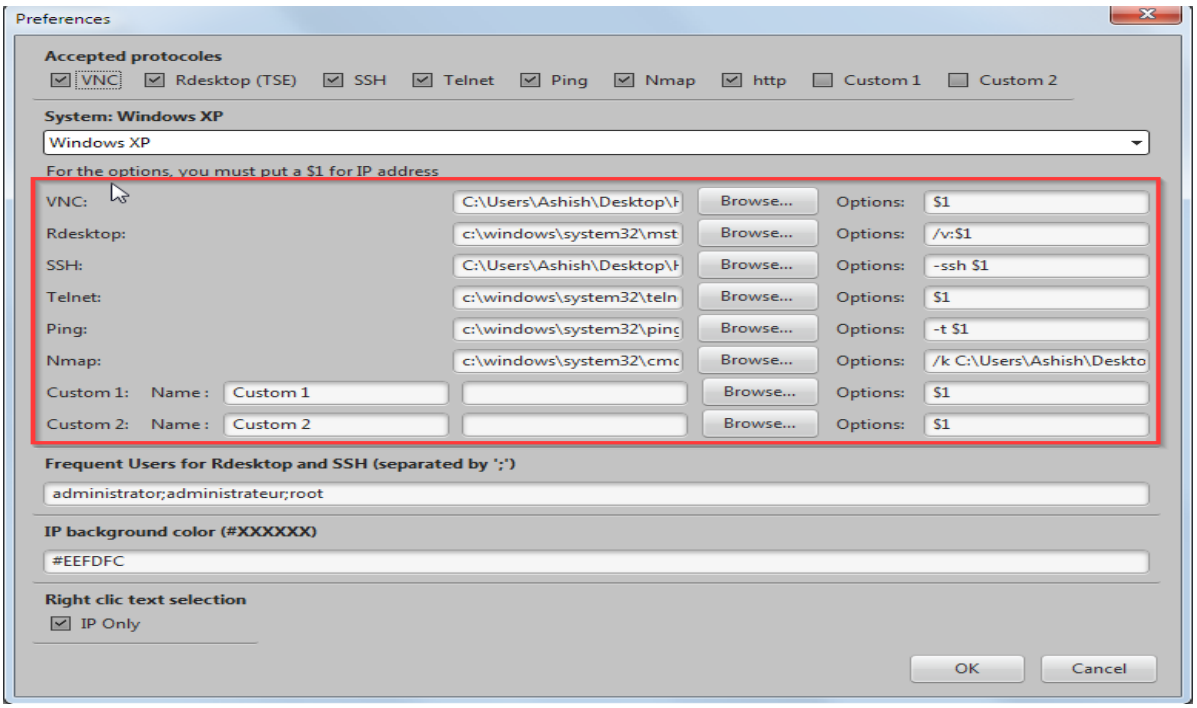


Figure 162: Configuring tools

Now as everything has been setup lets try to run it by,

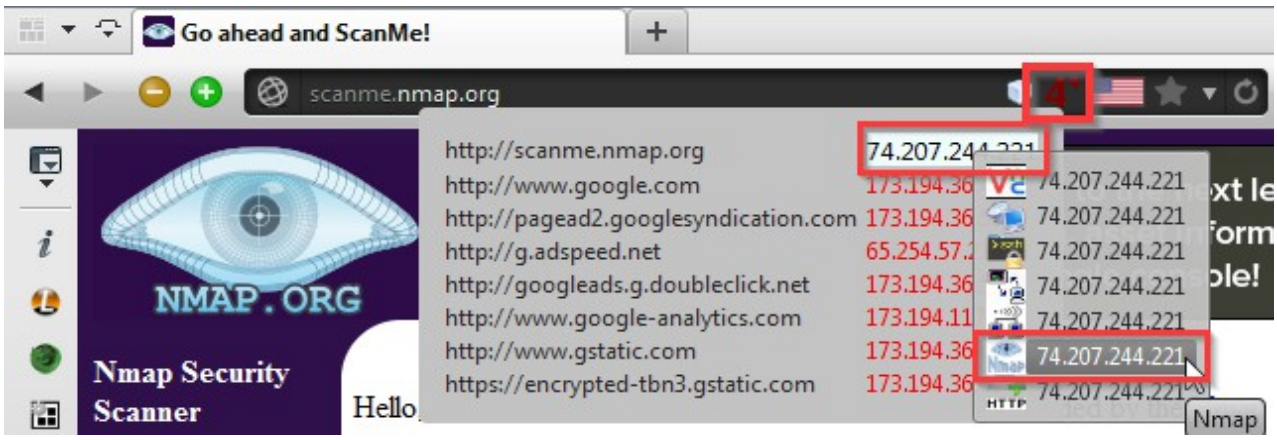


Figure 163: Using IPprotocols

clicking on red '4' icon from urlbar → click on the IP we want to target → click on the tool we want to use against that target IP, in this we have run nmap on scanme.nmap.org

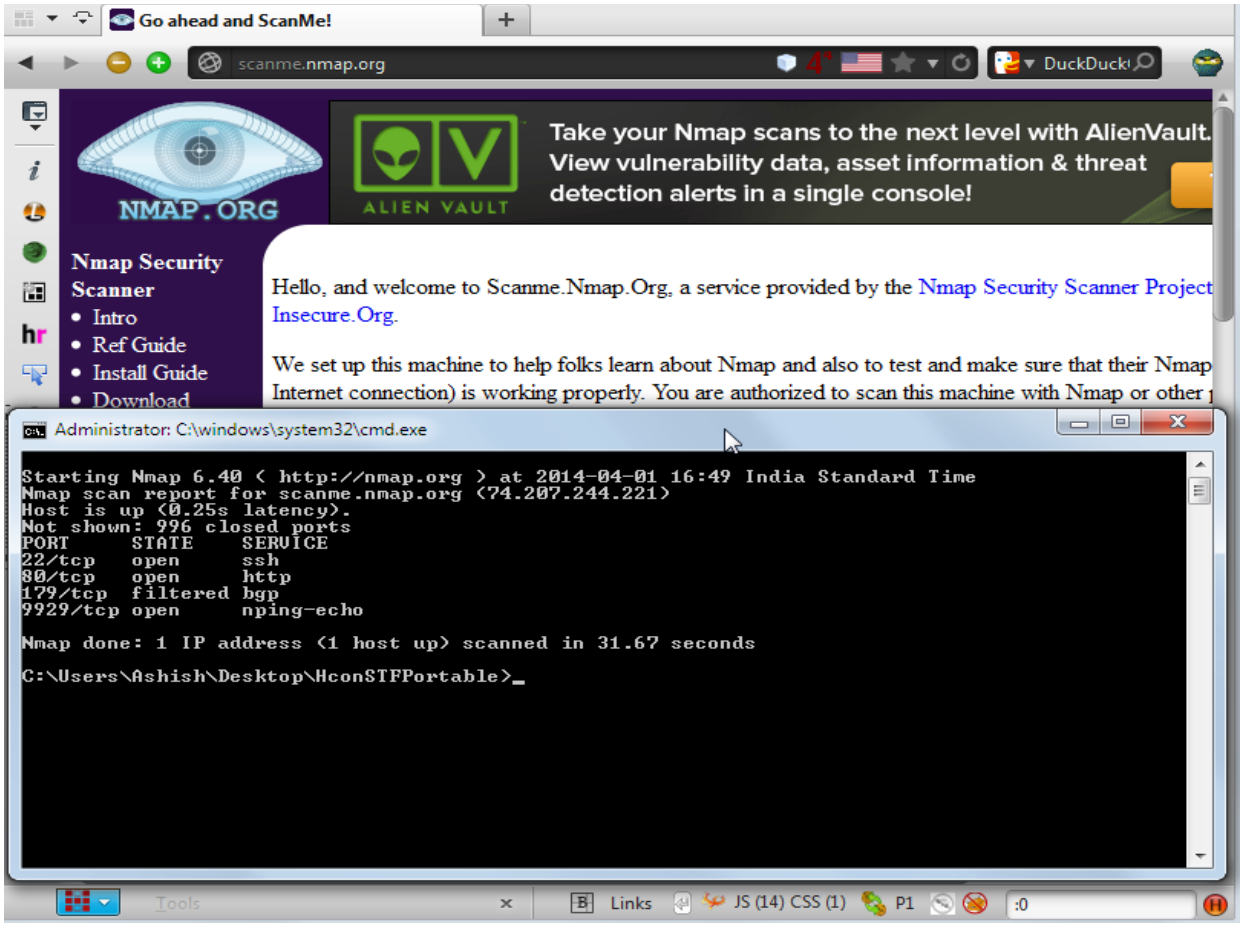

Go ahead and ScanMe!
scanme.nmap.org
NMAP.ORG
Take your Nmap scans to the next level with AlienVault.
View vulnerability data, asset information & threat detection alerts in a single console!
ALIEN VAULT
Nmap Security Scanner
Intro
Ref Guide
Install Guide
Download
Hello, and welcome to Scanme.Nmap.Org, a service provided by the Nmap Security Scanner Project Insecure.Org.
We set up this machine to help folks learn about Nmap and also to test and make sure that their Nmap Internet connection) is working properly. You are authorized to scan this machine with Nmap or other
Administrator: C:\windows\system32\cmd.exe
Starting Nmap 6.40 (http://nmap.org) at 2014-04-01 16:49 India Standard Time
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.25s latency).
Not shown: 996 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
179/tcp filtered bgp
9929/tcp open nping-echo
Nmap done: 1 IP address (1 host up) scanned in 31.67 seconds
C:\Users\Ashish\Desktop\HconSTFPortable>
Links
JS (14) CSS (1)
P1

Figure 164: Nmap results for scanme.nmap.org

Like this we can setup other tools or replace this default with our own favorite tools which takes IP address as target argument.

Note: *Once we have setup this tools and its preferences then we can use this on any IP address on the webpage or webapp we are testing.*

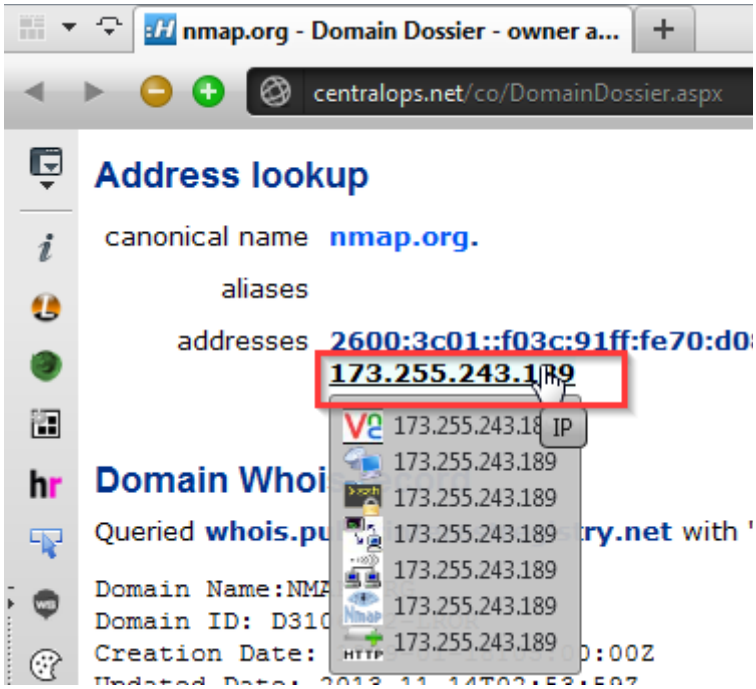


Figure 165: using IP address from webpage

Tools setup information:

- **UltraVNC**

  Download link: http://www.uvnc.com/downloads/

  Installation location: [absolute path to HconSTF DIR]\uvnc\vncviewer.exe

  download zip archive of the latest version compatible to our system.

- **Remote desktop**

  Download link: already installed in windows.

  Installation location: c:\windows\system32\mstsc.exe

- **Putty**

  Download link: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

  Installation location: [absolute path to HconSTF DIR]\tools\putty.exe

- **Telnet**

  Download link: already installed in windows.

  Installation location: c:\windows\system32\telnet.exe

- **Ping**

  Download link: already installed in windows.

  Installation location: c:\windows\system32\ping.exe

- **Nmap**

  Download link: http://nmap.org/download.html

  Installation location: [absolute path to HconSTF DIR]\tools\nmap\nmap.exe

nmap needs some dependencies to run properly under windows for that install the given installers from nmap directory,

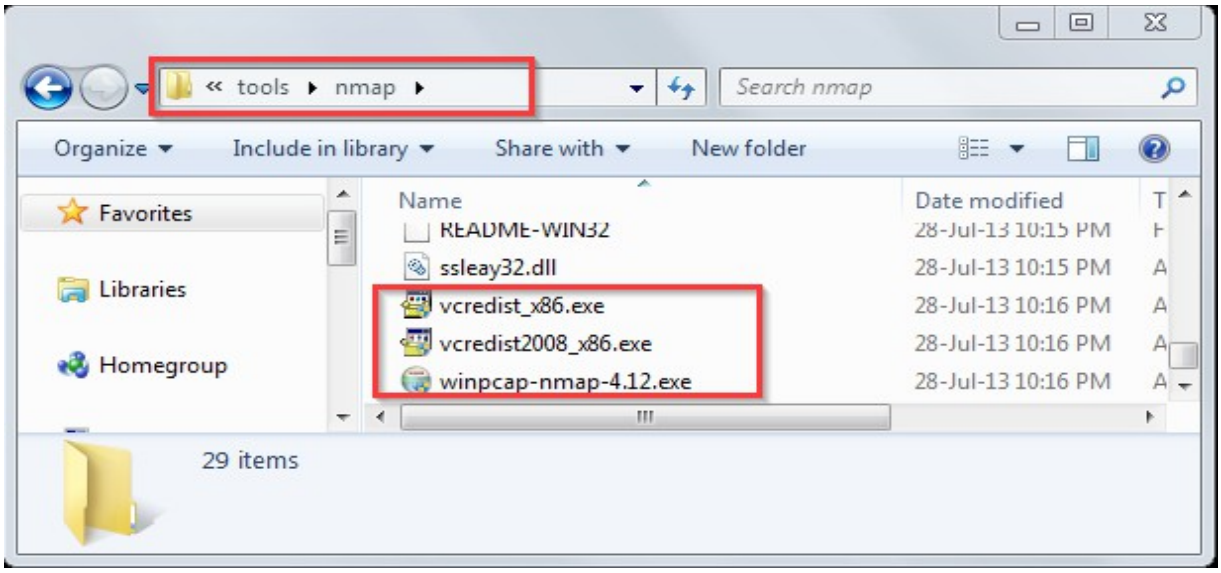


Figure 166: Nmap dependencies installers

Chapter 9: Troubleshooting

In this chapter we will look at troubleshooting most common user problems in HconSTF.

9.1 Tools Not Working from WebUI & Search Aggregator

The problem with this components of the Framework is that this are dependent on external web services which are online and which are not hosted nor maintained by Hcon.in so there are chances of it going offline and not found as the author of that online service change any link or components.

What we can do to fix it, is that you can notify us for the broken tool so in the next version we can fix it. and if you are an advance user then you can edit it or add your own plugin.

9.2 Missing Status Bar and H-menu

If the status bar is not there and is missing so we can't access Hmenu and other status bar tools.

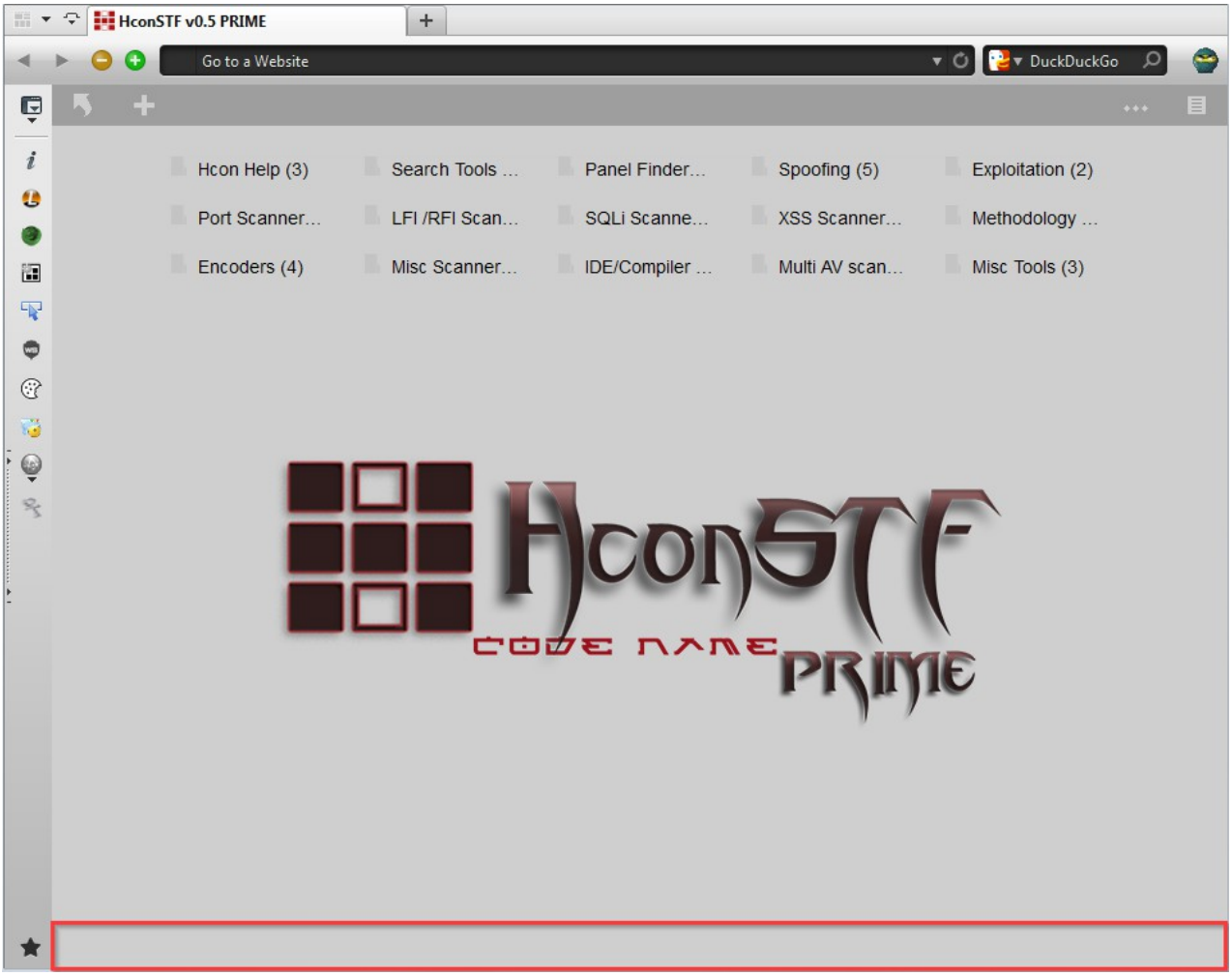


Figure 167: Hmenu and status bar missing

So to bring it back first try to close the HconSTF and run HconSTF cleaner and restart it, if it is still missing then follow this steps, right click on the fevicon area in URL bar → click on 'Add-on Bar'

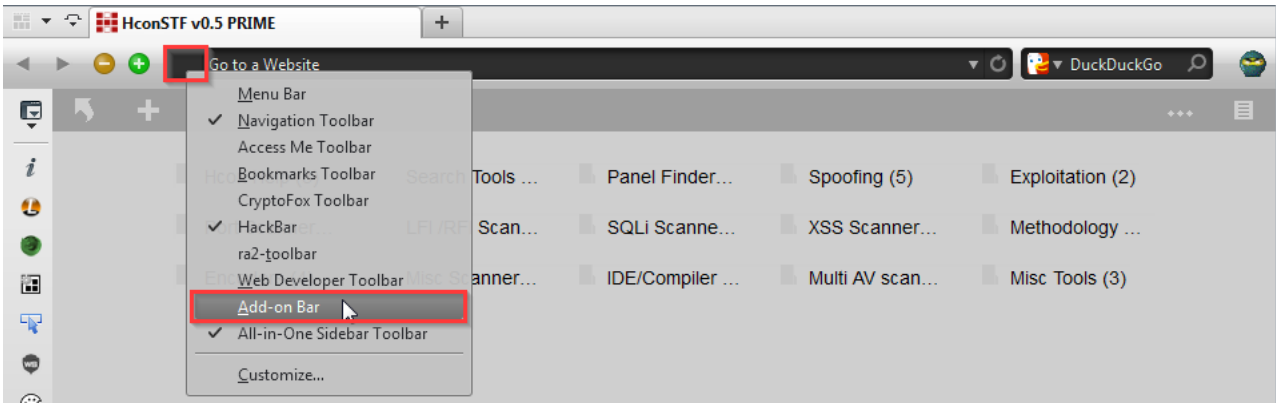


Figure 168: Select add-on bar

Now status bar and Hmenu is back.

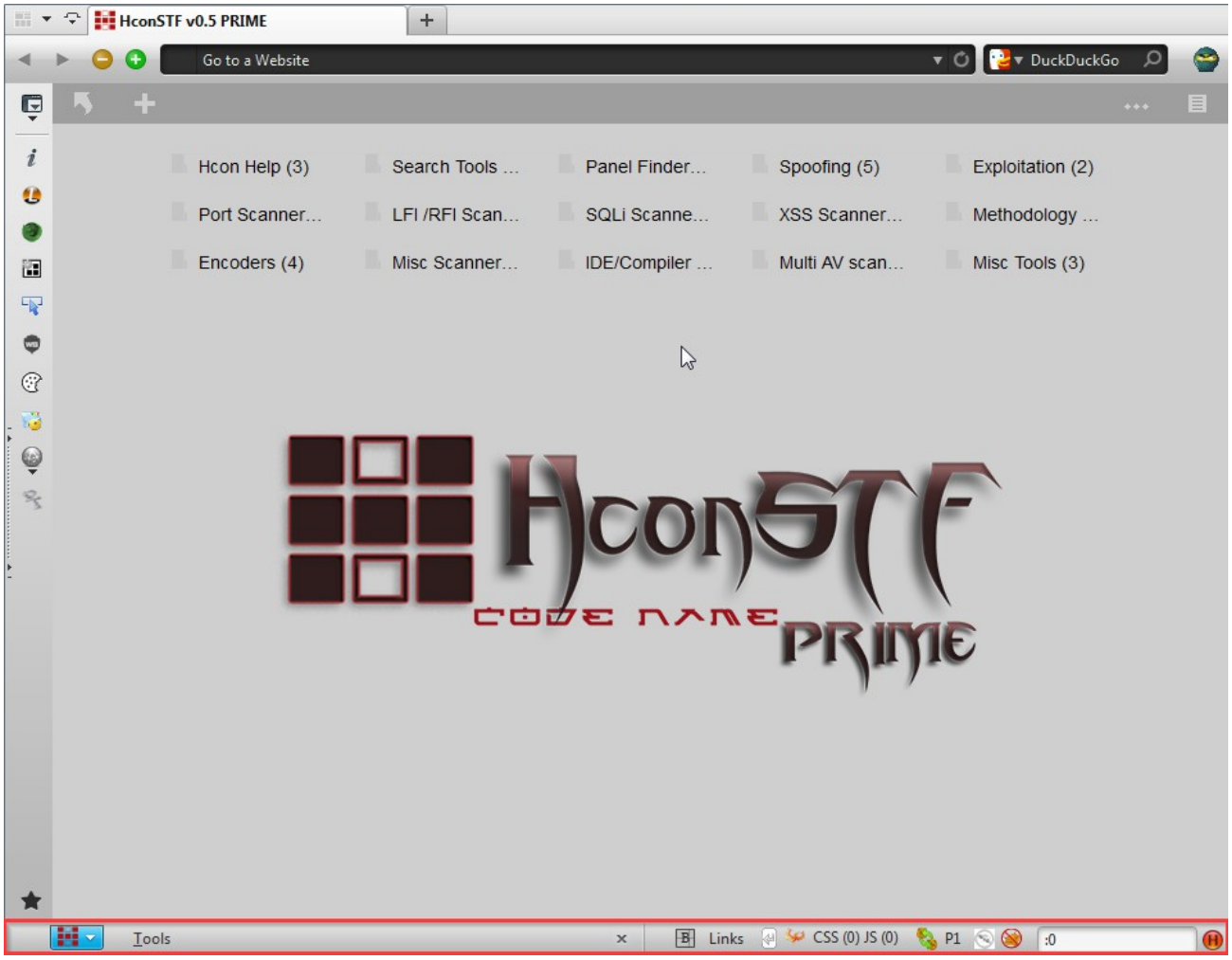


Figure 169: Hmenu and status bar restored

9.3 “Another Instance is Already Running” error

In windows many times after updating HconSTF or just restarting for any other task we are performing in HconSTF, it gives error which is related to that already one instance of HconSTF is running and it can not start it. For this just kill the HconSTF process via task manager and start the HconSTF using its launcher.

Chapter 10: Getting Further Information & Help

In this chapter we will look at way to get more information on HconSTF and contributing to it.

10.1 More Resources on HconSTF

Websites and links

For information on new versions and new updates

- HconSTF website: http://www.hcon.in/hconstf.html
- HconSTF news and updates: http://www.hcon.in/blog.html
- HconSTF Downloads: http://www.hcon.in/downloades.html
- Contact HconSTF developer: http://www.hcon.in/contact-us.html

Social Media

Connect with us on social media for frequent updates and quick tips on HconSTF

- Facebook: http://www.facebook.com/hcon.in
- Twitter: http://www.twitter.com/hconstf

Learning resources and get support

Get help for learning more about HconSTF and web application penetration testing

- HconSTF community forums: http://hcon.in/community.html
- For more tutorials and help documents: http://hcon.in/hconstf-docs.html

10.2 Contribute in HconSTF

Help us making it a strong community generated marvel, as community is heart of any Open source software, contribute back to security community.

Code - Develop - Test - Report

- Let us know if you have made any tool that can be integrated into HconSTF.
- Report us any bugs you find in HconSTF.

- Suggest any new tool/add-on/script that you think, that will help the community.
- Encountered a bug? you have a patch for it, share with us.

Share your knowledge to Community, make tutorials

- Make tutorials either videos or text + image.
- Join the forums and write informational post and help others about HconSTF.

Support us, spread the word

- Tell your friends and colleagues about HconSTF.
- Support us and share it on social media.

For more recent version of this information visit: http://www.hcon.in/contribute.html

10.3 Learn Web Application Pentesting with HconSTF

Learn the cutting edge techniques in webapp pentesting and expand your skills with Wab Application Pentesting with HconSTF (WAPH) course from Hcon.in by Ashish Mistry.

The course is available in two ways

- Fast-track workshop
- Full course with certification

Course dives from most basic to most advanced topics in Webapp Pentesting, with complete hands-on training materials.

For more details about the course contact us at: http://www.hcon.in/contact-us.html